Doktori értekezés

AMIKOR EGY SZORZAT KÉTFÉLEKÉPPEN ÁLL ELŐ

Pach Péter Pál

Matematika Doktori Iskola
Iskolavezető: Dr. Laczkovich Miklós, MTA tagja

Elméleti Matematika Doktori Program
Programvezető: Dr. Szűcs András, MTA levelező tagja

Témavezető: Dr. Szabó Csaba, egyetemi tanár, MTA doktora

Eötvös Loránd Tudományegyetem
Természettudományi Kar, Algebra és Számelmélet Tanszék

Budapest, 2012.

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek, Szabó Csabának az érdekes problémafelvetéseket, a közös kutatást, az értekezés alapos ellenőrzését, értékes észrevételeit és megjegyzéseit, valamint minden egyéb segítséget, melyet az elmúlt években kaptam tőle.
Köszönöm a közös munkát Maga Péternek, Pluhár Gabriellának és Pongrácz Andrásnak.
Nagyon hálás vagyok Sárközy Andásnak, aki érdekes problémákra hívta fel a figyelmem, és az ezekből született cikkek elkészítésében is nagy segítséget nyújtott.
Köszönet illeti még Balog Antalt és Győri Ervint, akik számos fontos cikket, könyvet, eredményt ajánlottak figyelmembe, melyek nélkülözhetetlenek voltak a témák alapos megismerésében és kutatásában.
Köszönöm gimnáziumi matematika tanáraimnak: Fazakas Tündének, Hraskó Andrásnak és Surányi Lászlónak, hogy megismertették velem a matematikát, és elmélyítették annak szeretetét.
Végül, de nem utolsó sorban szeretném megköszönni családomnak a támogatást és biztatást, amit kaptam tőlük.

Tartalomjegyzék

1. fejezet

Bevezetés

Kutatásaink során több számelméleti problémával is foglalkoztunk, és ezek nagy részében fontos szerepet játszott, hogy bizonyos halmazokban hány elem áll elő pontosan egyféleképpen, mint szorzat. Ezek az egyféleképpen előállítható szorzatok a legkülönbözőbb környezetekben kerültek elő. Az is eltérő volt, hogy mit nevezünk különbözőnek, például volt olyan, amelynél ab és ba egyformának számított, volt, ahol különbözőnek. Abban is különböznek a kérdések, hogy két, vagy több tényezős szorzatokat vizsgáltunk, de mindig kiemelt szerepet játszott azon elemek halmaza, amelyek pontosan egyféleképpen álltak elő szorzatként. Most röviden bemutatjuk a dolgozat eredményeit, azonban azok különbözősége miatt az előzményeket és a szükséges hátteret fejezetenként ismertetjük.

A 2. fejezetben Pilz egy kódelméleti eredetű sejtését igazoljuk. Pilz azt vizsgálta, hogy mi a minimális távolsága a következő módon definiált kódnak: legyen $f = x^n + x^{n-1} + \cdots + x$, és legyen $C(f,k)$ az a lineáris kód, melyet az $f \circ x$, $f \circ x^2$, ..., $f \circ x^k$ polinomok generálnak. Pilz azt sejtette, hogy ennek a kódnak a minimális távolsága n. Ez a kérdés az alábbi tisztán számelméleti kérdéssel ekvivalens: igaz-e tetszőleges $K \subseteq \mathbb{N}$ véges halmaz esetén, hogy legalább n olyan szám van, amely páratlan sokféleképpen áll elő egy K-beli és egy $\{1,2,\ldots,n\}$-beli szám szorzataként? Pilz sejtése szerint az ilyen tulajdonságú számok száma mindig legalább n. Azt tapasztaljuk, hogy azok között a számok között, melyek páratlan sokféleképpen állnak elő szorzatként, legtöbbször dominálnak azok, melyek pontosan egyféleképpen állnak elő. Ennek segítségével megjavítjuk Pilz a kód minimális távolságára vonatkozó $(\pi(n)+2)$-es alsó becslését, és igazoljuk, hogy a kód minimális távolsága legalább $\frac{n}{(\log n)^{\lambda}}$, ahol $\lambda \approx 0,223$. Pilz 123-sejtés néven a

$K = \{1, 2, \ldots, k\}$ esetre külön megfogalmazta a problémát. Mi igazoljuk ezt a sejtést, azaz megmutatjuk, hogy legalább n elem páratlan sokszor szerepel az $\{1, 2, \ldots, n\} \cdot \{1, 2, \ldots, k\}$ multihalmazban. A fejezet eredményei [29]-ben jelentek meg. Érdemes megjegyezni, hogy ez utóbbi sejtést velünk egy időben Huang, Ke és Pilz is igazolták, dolgozatuk az AMS Proceedings-ben jelent meg [22].

A 3. fejezetben egy más jellegű témával foglalkozunk. Egyenletek megoldhatóságára vonatkozó Ramsey-típusú és sűrűségi tételeket igazolunk. Pomerance és Schinzel [33] bebizonyították, hogy a négyzetmentes számok tetszőleges 2-színezése esetén van monokromatikus megoldása az $ab = c$ egyenletnek, és megkérdezték, hogy ez tetszőleges r-színezés esetén is igaz-e. Mi ezt ennél lényegesen általánosabban bizonyítjuk: igazoljuk, hogy tetszőleges $k \geq 2, l, r$ számok esetén az $a_1 \ldots a_k = b_1 \ldots b_l$ egyenletnek van monokromatikus megoldása a négyzetmentes számok tetszőleges r-színezése esetén. Továbbá megmutatjuk, hogy sűrűségi tétel pontosan akkor teljesül, ha $k = l$. Tehát $k \neq l$ esetén elképzelhető, hogy egy „sűrű" halmaz elemeiből képzett egyik k-as szorzat sem egyenlő a halmaz elemeiből képzett egyik l-es szorzattal sem. Viszont, ha a természetes számokat véges sok színnel színezzük, akkor már biztosan lesz olyan szám, amely egyforma színű elemekből képzett k-as és l-es szorzataként is előáll. A fejezet eredményeit [26] tartalmazza.

A 4. fejezetben szorzatokat szeretnénk összegként előállítani, pontosabban az $a_1 + \cdots + a_n = cd$ és $ab + 1 = cd$ egyenleteket vizsgáljuk $\mathbb{Z}_m$-ben. Csikvári, Gyarmati és Sárközy [6] megkérdezték, hogy az $a + b = cd$, illetve az $ab + 1 = cd$ egyenletek esetén igazolható-e Ramsey-típusú tétel $\mathbb{Z}_m$-ben. Vagyis igaz-e, hogy ha a színek r számát rögzítjük, akkor elegendően nagy m esetén $\mathbb{Z}_m$ tetszőleges r-színezése esetén van monokromatikus megoldása az $a + b = cd$, illetve $ab + 1 = cd$ egyenleteknek. Mi egy ennél általánosabb eredményt igazolunk: megmutatjuk, hogy tetszőleges $n, r \in \mathbb{N}$ esetén igaz, hogy ha m elegendően nagy, akkor $\mathbb{Z}_m$ tetszőleges r-színezése esetén van monokromatikus megoldása az $a_1 + \cdots + a_n = cd$ egyenletnek. Valamint az $ab + 1 = cd$ egyenlet esetén ellenpéldát adunk: már 2 szín esetén is végtelen sok olyan m létezik, melyre $\mathbb{Z}_m$-nek van olyan 2-színezése, hogy az $ab + 1 = cd$ egyenletnek nincs monokromatikus megoldása. Ellenpéldánk akkor működik, ha n-nek van kicsi prímosztója. Azt sejtjük, hogy ez az egyetlen akadálya egy Ramsey-típusú tétel bizonyításának. Megmutatjuk, hogy ha m olyan négyzetmentes szám, melynek nincsen „kicsi" prímosztója, valamint az $r \sum_{p|m} \frac{1}{p^{1/4}} \leq \frac{1}{\sqrt{10}}$ feltétel is teljesül, akkor $\mathbb{Z}_m$ tetszőleges r-színezése esetén van monokromatikus megoldása az $ab+1=cd$ egyenletnek. A fejezet eredményei [27]-ben olvashatók.

Végül, az utolsó fejezetben általánosított multiplikatív Sidon-sorozatokkal foglalkozunk, mint a neve is mutatja, itt szorzatok egyféleképpen való előállíthatóságát vizsgáljuk. Erdős [9] igazolta, hogy az $\{1,2,\ldots,n\}$ halmaznak kiválasztható $\pi(n)+c_1n^{3/4}/(\log n)^{3/2}$ sok eleme úgy, hogy az ezekből képezett kettes szorzatok mind különbözők. Azt is bizonyította, hogy egy ilyen tulajdonságú halmaz elemszáma legfeljebb $\pi(n)+c_2n^{3/4}$ lehet, majd 31 évvel később [11]-ben ezt a felső becslést $\pi(n)+c_2n^{3/4}/(\log n)^{3/2}$-re javította. Mi ennek általánosításaként igazoljuk, hogy kiválasztható $\pi(n)+\pi(n/2)+c\frac{n^{2/3}}{(\log n)^{4/3}}$ elem úgy, hogy az $s_1s_2s_3=t_1t_2t_3$ egyenletnek ne legyen páronként különböző számokból álló megoldása. Azonban ha legalább $\pi(n)+\pi(n/2)+\left(\frac{2e}{3}+\varepsilon\right)\cdot n^{2/3}\cdot\frac{\log n}{\log\log n}$ elemet választunk ki, akkor már biztosan lesz különböző számokból álló megoldás. Az $s_1s_2s_3s_4=t_1t_2t_3t_4$ egyenlet esetén $\pi(n)+n^{3/5}/(\log n)^{6/5}$-ös alsó és $\pi(n)+(10+\varepsilon)n^{2/3}$-os felső becslést igazolunk. Ezek következményeként megjavítjuk Erdős, Sárközy, T. Sós és Győri eredményeit, akik azt vizsgálták, hogy legfeljebb hány szám választható ki úgy, hogy közülük semelyik k-nak a szorzata ne legyen négyzetszám. Bizonyították, hogy ha $8\le k$ egy 4-gyel osztható szám, akkor egy ilyen halmaz elemszáma legfeljebb $\pi(n)+cn^{3/4}/(\log n)^{3/2}$ lehet. Mi ezt a felső becslést $\pi(n)+cn^{2/3}$-ra javítjuk. Amikor $4\le k$ szám 4-es maradéka 2, akkor Erdős, Sárközy, T. Sós [12] és Győri [18] eredménye szerint a maximális elemszám legfeljebb $\pi(n)+\pi(n/2)+cn^{2/3}\log n$. Mi a felső becslés hibatagján egy $\log\log n$-es faktort javítunk, megmutatjuk, hogy a halmaz elemszáma legfeljebb $\pi(n)+\pi(n/2)+cn^{2/3}\log n/\log\log n$.

2. fejezet

Minimális távolság és páratlan sokféleképpen előálló szorzatok

Ebben a fejezetben egy majdnemgyűrű-kód minimális távolságát vizsgáljuk. Egy majdnemgyűrű egy olyan kétműveletes algebrai struktúra, amely teljesíti a gyűrűaxiómákat, kivéve az összeadás kommutativitását, és a disztributivitások közül is csak az egyiket követeljük meg. Például a polinomok majdnemgyűrűt alkotnak, ahol az összeadás a polinom összeadás, a szorzás pedig a polinomok kompozíciója. Ebben a példában az összeadás kommutatív, viszont csak a jobb oldali disztributivitás teljesül. A majdnemgyűrűk fontos szerepet játszanak a kombinatorikában: segítségükkel blokkrendszereket és hatékony hibajavító kódokat lehet konstruálni. Bővebb leírás ezekről a kódokról [8]-ban, [30]-ban és [31]-ben található. Pilz egy speciális és nagyon érdekes majdnemgyűrű kódot vizsgált, melynek definíciója a következő: legyen $f \in \mathbb{Z}_2[x]$ egy polinom, és legyen $C(f,k)$ az a lineáris kód, amelyet az $f \circ x$, $f \circ x^2$, ..., $f \circ x^k$ polinomok generálnak. Az f polinom fokát jelölje n. Könnyen meggondolható, hogy $C(f,k)$ lineáris kód hossza nk, dimenziója pedig k.

A kódok egyik legfontosabb paramétere a kódszavak közötti minimális távolság. Ha C lineáris kód, akkor a minimális távolság megegyezik a legkisebb súlyú nemnulla kódszó súlyával, jelöljük ezt $w(C)$-vel. Ha $f \in C(f,k)$, akkor f súlya az f polinom nemnulla együtthatóinak száma. Pilz az $f = x^n + x^{n-1} + \cdots + x$ polinom által definiált kódot vizsgálta. A tapasztalat azt mutatta, hogy ennek minimális távolsága n. Ennél nagyobb nem lehet, hiszen az $f \circ x$ polinom súlya n.

Egy $\mathbb{Z}_2$ feletti polinomot egyértelműen megadhatunk a nemnulla együtthatójú tagok kitevőinek sorozatával. Ha például az f polinom $f = x^{a_1} + \cdots + x^{a_l}$ alakú, ahol $1 \leq a_1 < \cdots < a_l = n$, akkor f-et az $(a_1, \ldots, a_l)$ számsorozattal adjuk meg. Az f polinom és x^j kompozíciója $f \circ x^j = x^{ja_1} + \cdots + x^{ja_l}$, tehát az $f \circ x^j$ polinomhoz tartozó számsorozat $(ja_1, \ldots, ja_l)$, ezt úgy is megkaphatjuk, hogy f kitevő-sorozatának minden tagját megszorozzuk j-vel. Vizsgáljuk meg, hogyan kapjuk meg $C(f, k)$ minimális távolságát. A nemnulla kódszavak úgy kaphatók, hogy vesszük az $f \circ x$, $f \circ x^2$, ..., $f \circ x^k$ polinomok egy nemnulla lineáris kombinációját, és mivel $\mathbb{Z}_2$ felett vagyunk, ez közülük néhánynak az összege, például $f \circ x^{b_1} + \cdots + f \circ x^{b_m}$. Ha $f = x^n + x^{n-1} + \cdots + x$, akkor $f \circ x^{b_1}$, ..., $f \circ x^{b_m}$ polinomok kitevő-sorozata rendre $(b_1, 2b_1, \ldots, nb_1)$, ... , $(b_m, 2b_m, \ldots, nb_m)$. Így $w(f \circ x^{b_1} + \ldots + f \circ x^{b_m})$ értékét az adja meg, hogy az ib_j alakú számokat véve $1 \leq i \leq n$, $1 \leq j \leq m$ esetén hány olyan szám van, amely közöttük páratlan sokszor szerepel. A kérdés az, hogy mely olyan b_1, ..., b_m kitevő-sorozatra lesz a páratlan sokszor megkapott számok száma minimális, ahol $1 \leq b_1 < \ldots < b_m \leq k$.

Tehát a kérdést a következő módon is megfogalmazhatjuk: legyenek $N = \{1, 2, \ldots, n\} = \underline{n}$ és $K \subseteq \mathbb{N}$ véges halmazok. Az összes lehetséges módon összeszorzunk egy-egy N-beli és K-beli elemet, így kapunk $n \cdot |K|$ darab számot. Ezek közül bizonyosakat páros, bizonyosakat páratlan sokszor kapunk meg. A kérdés az, hogy (legalább) hány olyan szám lesz, amelyet páratlan sokszor kapunk meg. Vezessük be a következő jelölést. A pozitív egész számok két véges részhalmazára, A-ra és B-re legyen

$$A * B = \{ab \mid a \in A, b \in B \text{ és } ab \text{ páratlan sokszor szerepel } A \cdot B\text{-ben}\}.$$

Azaz, ha $A = \{a_1, \ldots, a_k\}$, akkor $A * B = a_1 B \Delta \cdots \Delta a_k B$, ahol Δ a szimmetrikus differenciát jelöli. Az $A * B$ halmaz pontosan azokat a számokat tartalmazza, amelyek páratlan sokféleképpen állnak elő egy A-beli és egy B-beli szám szorzataként.
Pilz a következő sejtéseket fogalmazta meg:

2.1. Sejtés. (123-sejtés) Ha n, k pozitív egész számok, akkor $|\underline{n} * \underline{k}| \geq n$.

2.2. Sejtés. Ha n pozitív egész szám, és $K \subset \mathbb{N}$ véges, akkor $|\underline{n} * K| \geq n$.

Ha N-ről nem követelnénk meg, hogy $N = \underline{n}$ teljesüljön valamely n természetes számra, hanem a természetes számok tetszőleges véges részhalmaza lehetne, akkor már nem igaz, hogy legalább $|N|$ számot kapunk meg páratlan sokszor. Nem igaz, hogy tetszőleges $K, N \subseteq \mathbb{N}$ véges halmazokra

$|K * N| \geq \max(|K|, |N|)$. Tekintsük ugyanis a következő példát:

$$K = \{1, a\} \text{ (ahol } 1 < a \text{ egész)}, \; N = \{1, a, a^2, \ldots, a^{n-1}\}.$$

Ebben az esetben a $K \cdot N$-beli szorzatok $1, a, a^2, \ldots, a^{n-1}, a, a^2, \ldots, a^n$, vagyis $K * N = \{1, a^n\}$, tehát $|K * N| = 2$.

Sőt, $|K * N| \geq \min(|K|, |N|)$ sem igaz, mint azt a következő ellenpélda mutatja: $K = \{2^1, 2^2, 2^4, \ldots, 2^{2^n}\}, N = \{1\} \cup K$. Ekkor

$$K * N = K * (\{1\} \cup K) = K\Delta(K * K) =$$
$$= \{2^1, 2^2, 2^4, \ldots, 2^{2^n}\}\Delta\{2^2, 2^4, 2^8, \ldots, 2^{2^{n+1}}\} = \{2^1, 2^{2^{n+1}}\},$$

és így $|K*N| = 2$. Tehát $2 \leq |K*N|$-nél több nem igaz, ez viszont mindig teljesül a triviális $|K| = |N| = 1$ eset kivételével, hiszen $a = \min\limits_{i \in K} i, b = \min\limits_{j \in N} j, c = \max\limits_{i \in K} i, d = \max\limits_{j \in N} j$ esetén könnyen láthatóan ab-t és cd-t csak egyszer-egyszer kapjuk meg K-beli és N-beli elemek szorzataként, valamint $ab \neq cd$.

Számos példa van, amikor $|\underline{n} * K| = n$ teljesül. Például $\underline{n} * \{1\} = \underline{n}$, illetve $\underline{n} * \underline{n} = \{1^2, 2^2, \ldots, n^2\}$. További példákat kaphatunk a probléma egy újabb megközelítése segítségével. Először minden pozitív egész számhoz egy $\mathbb{Z}_2$ feletti monomot rendelünk a következő módon. A prímszámokhoz különböző változókat rendelünk: p-hez x_p-t. Ha az m szám kanonikus alakja $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, akkor m-hez az $x_{p_1}^{\alpha_1} \ldots x_{p_r}^{\alpha_r}$ monomot rendeljük. (Az 1-hez az 1-et rendeljük.) A pozitív egész számok egy véges részhalmazához az elemeihez rendelt monomok összegét rendeljük. Az A halmazhoz rendelt polinomot jelölje f_A, például $A = \{1, 2, 3, 4\}$ esetén $f_A = 1 + x_2 + x_3 + x_2^2$. Az f_A polinomban a tagok száma $|A|$, valamint $f_{A*B} = f_A \cdot f_B$ teljesül. Mivel $\mathbb{Z}_2$ felett vagyunk, ezért minden összeget tagonként kell négyzetre emelni, így tetszőleges r esetén $f_A^{2^r}$ tagjainak száma szintén $|A|$. Például $r = 2$ választással $f_{\{1,2,3,4\}}^4 = 1 + x_2^4 + x_3^4 + x_2^8$. Az $f_A^{2^r} = f_A \cdot f_A^{2^r - 1}$ összefüggés segítségével újabb konstrukciókat nyerhetünk $|\underline{n} * K| = n$-re: például, $f_{\{1,2,3,4\}}^3 = 1 + x_2 + x_3 + x_2^3 + x_3^2 + x_2^2 x_3 + x_2 x_3^2 + x_3^3 + x_2^5 + x_2^2 x_3^2 + x_2^4 x_3 + x_2^6$ egyenlőségből $\{1, 2, 3, 4\} * \{1, 2, 3, 8, 9, 12, 18, 27, 32, 36, 48, 64\} = \{1, 16, 81, 256\}$ adódik.

Több esetben a páratlan sokszor szereplő szorzatok számát a pontosan egyszer szereplők számával becsüljük alulról. Ez indokolja a következő jelölés bevezetését. Legyenek $K, N \subseteq \mathbb{N}$ véges halmazok. A $K \cdot N$ halmaz azon elemeinek halmazát, amelyek egyféleképpen állnak elő egy K-beli és egy N-beli elem szorzataként, jelölje $1(K, N)$.

A fejezetben először az általános esettel fogunk foglalkozni. Pilz megmutatta, hogy $|\underline{n} * K| \geq \pi(n) + 2$ teljesül $n \geq 4$ esetén, mi ezt az eredményt megjavítva a 2.2. Tételben bebizonyítjuk, hogy $|\underline{n} * K| \geq \frac{cn}{(\log n)^\lambda}$ is fennáll, ahol $c > 0$ és $\lambda \approx 0,223$. Pontosabban azt is igazoljuk, hogy már az egyféleképpen előálló szorzatok $|1(\underline{n}, K)|$ számára is fennáll ez az alsó becslés.

Ezután a 2.3. Tételben bizonyítjuk az 123-sejtést, azaz igazoljuk, hogy $|\underline{n} * \underline{k}| \geq n$ mindig teljesül. A bizonyítás során több esetet különböztetünk meg aszerint, hogy k mekkora. Érdemes megjegyezni, hogy ez utóbbi sejtést velünk egy időben Huang, Ke és Pilz is igazolták. Dolgozatuk az AMS Proceedings-ben jelent meg [22]. A fejezet eredményei [29]-ben jelentek meg.

2.1. Alsó becslés

A bevezetésben ismertettünk bizonyos lineáris kódokat, melyek minimális távolságát a következő függvénnyel tudjuk alulról becsülni:

$$g(n) = \min_{K \subseteq \mathbb{N}, |K| < \infty} |\underline{n} * K|,$$

ahol n pozitív egész szám. A minimális távolságra, vagyis g-re keresünk minél jobb alsó becslést.

A $|K| = 1$ esetben például $|\underline{n} * K| = n$, hiszen K egyetlen elemét a-val jelölve $\underline{n} * K = \{a, 2a, ..., na\}$. Ebből következik, hogy minden n természetes számra érvényes a $g(n) \leq n$ egyenlőtlenség.

Pilz [32] igazolta, hogy $g(n) \geq \pi(n) + 2$. A bizonyításból az is kiderül, hogy $\underline{n} \cdot K$-ban legalább $\pi(n) + 2$ olyan elem van, amely pontosan egyféleképpen áll elő egy $\underline{n}$-beli és egy K-beli elem szorzataként. Az $\underline{n} \cdot K$ szorzatban pontosan egyszer szereplő elemek halmazának minimális elemszámát jelölje $g_1(n) = \min_{K \subseteq \mathbb{N}, |K| < \infty} |1(\underline{n}, K)|$. A célunk g_1-re minél jobb alsó becslést adni, ezzel egyben g-re is érvényes alsó becslést nyerünk, hiszen $g_1(n) \leq g(n)$. A bizonyításunk a következő észrevételen alapul:

2.1. Állítás. *Minden n természetes számra*

$$g_1(n) \geq \sum_{\sqrt{n} < p \leq n} g_1\left([n/p]\right),$$

ahol az összegzés a $(\sqrt{n}, n]$ intervallumba eső prímekre történik.

Bizonyítás. Legyen $p \in (\sqrt{n}, n]$ prímszám és $K_p \subseteq K$ azon K-beli elemek halmaza, amelyek prímtényezős felbontásában p kitevője maximális. Ehhez hasonlóan legyen $\underline{n}_p \subseteq \underline{n}$ azon $\underline{n}$-beli elemek halmaza, amelyek prímtényezős felbontásában p kitevője maximális. A p prímszám kitevőjét vizsgálva látható, hogy ha

$$ab = cd \text{ (ahol } a \in \underline{n}_p, b \in K_p, c \in \underline{n}, d \in K),$$

akkor $c \in K_p$ és $d \in \underline{n}_p$ is teljesül. Belátjuk, hogy $p, q \leq n$ különböző prímszámok esetén az $\underline{n}_p \cdot K_p$ és az $\underline{n}_q \cdot K_q$ halmazok diszjunktak. Logikai szimmetria miatt feltehető, hogy $p < q$. A p prímszám kitevőjét vizsgálva megállapíthatjuk, hogy

$$(\underline{n}_p \cdot K_p) \cap (\underline{n}_q \cdot K_q) \neq \emptyset$$

csak úgy lehetséges, ha $\underline{n}_p \cap \underline{n}_q \neq \emptyset$. Azonban $d \in \underline{n}_p \cap \underline{n}_q$ esetén a d szám $d = pqd'$ alakban írható, így

$$\bar{d} = p^2 d' < d$$

olyan eleme $\underline{n}$-nek, amelyben p kitevője nagyobb, mint d-ben, ami ellentmondás.

Az eddigiekből következik az alábbi egyenlőtlenség:

$$|1(\underline{n}, K)| \geq \sum_{\sqrt{n} < p \leq n} |1(\underline{n}_p, K_p)|. \tag{2.1}$$

Mivel $\sqrt{n} < p \leq n$, ezért $\underline{n}$-nek van p-vel osztható eleme, de nincs olyan, ami p^2-tel is osztható lenne, ezért

$$\underline{n}_p = \{p, 2p, ..., [n/p]p\}.$$

Könnyen látható, hogy

$$|1(\underline{n}_p, K_p)| = |1(\underline{[n/p]}, K_p)|,$$

így g_1 definícióját felhasználva azt kapjuk, hogy:

$$|1(\underline{n}_p, K_p)| = |1(\underline{[n/p]}, K_p)| \geq g_1([n/p]).$$

Ezt (2.1)-gyel egybevetve a kívánt

$$g_1(n) \geq \sum_{\sqrt{n} < p \leq n} g_1([n/p])$$

egyenlőtlenséget kapjuk. □

A tétel, amit bizonyítunk, a következő:

2.2. Tétel. *Minden $\lambda > \lambda_0$ esetén létezik olyan $c = c(\lambda) > 0$, hogy minden $n > 1$ esetén*

$$g_1(n) \geq c \cdot \frac{n}{\log^\lambda n}, \tag{2.2}$$

ahol λ_0 a következő egyenlet megoldása:

$$\int_0^1 \left(\frac{2}{y}\right)^{\lambda_0} \frac{1}{2-y} dy = 1.$$

Az integrálegyenletből kapott λ_0 értékére $\lambda_0 \approx 0,223$.

Bizonyítás. Rögzítsünk egy $1 > \lambda > \lambda_0$ számot. Azt állítjuk, hogy létezik olyan $c > 0$ konstans, melyre a (2.2) egyenlőtlenség fennáll minden $n > 1$ esetén. Az állítást n-re vonatkozó teljes indukcióval bizonyítjuk. Először az indukciós lépést vizsgáljuk meg. Tegyük fel, hogy (2.2) teljesül minden $n < m$ esetén. Most megmutatjuk, hogy $n = m$ esetén is teljesül. A c konstans értékét később választjuk meg. A 2.1. Állítást és az indukciós feltevést használva a következő becslést kapjuk:

$$\begin{aligned} g_1(m) &\geq \sum_{\sqrt{m}<p\leq m} g_1(\lfloor m/p \rfloor) \geq \sum_{\sqrt{m}<p\leq m} c \cdot \frac{\lfloor m/p \rfloor}{\log^\lambda(\lfloor m/p \rfloor)} \geq \\ &\geq \sum_{\sqrt{m}<p<m/2} c \cdot \frac{\lfloor m/p \rfloor}{\log^\lambda(\lfloor m/p \rfloor)} \geq \sum_{\sqrt{m}<p<m/2} c \cdot \frac{m/p - 1}{\log^\lambda(\lfloor m/p \rfloor)} = \\ &= \sum_{\sqrt{m}<p<m/2} c \cdot \frac{m/p}{\log^\lambda(\lfloor m/p \rfloor)} - \sum_{\sqrt{m}<p<m/2} c \cdot \frac{1}{\log^\lambda(\lfloor m/p \rfloor)}. \end{aligned} \tag{2.3}$$

Rosser és Schoenfeld [37] igazolták, hogy $\pi(m) < \frac{1,25506m}{\log m}$ minden $m > 1$ esetén fennáll, így

$$\pi(m/2) - \pi(\sqrt{m}) \leq \pi(m) < 1,5 \cdot \frac{m}{\log m}.$$

Ennek segítségével megbecsüljük (2.3) utolsó sorának második tagját:

$$\begin{aligned} \sum_{\sqrt{m}<p<m/2} c \cdot \frac{1}{\log^\lambda(\lfloor m/p \rfloor)} &\leq \sum_{\sqrt{m}<p<m/2} c \cdot \frac{1}{(\log 2)^\lambda} \leq \\ &\leq 1,5 \cdot \frac{m}{\log m} \cdot \frac{c}{\log 2} = o\left(\frac{m}{\log^\lambda m}\right), \end{aligned} \tag{2.4}$$

ugyanis $\lambda < 1$.

Most a fő tag becslésével folytatjuk. Mertens nevezetes tétele szerint létezik létezik olyan pozitív M szám, hogy

$$\sum_{p \le x} \frac{1}{p} = \log\log x + M + o(1).$$

Így minden $\varepsilon > 0$-hoz létezik $B = B(\varepsilon)$, hogy $B \le a \le b$ esetén

$$\left| \sum_{a < p \le b} \frac{1}{p} - \log\log b + \log\log a \right| < \varepsilon \tag{2.5}$$

teljesül. Ha $m > 2^{2K}$, akkor $m^{\frac{1}{2}+\frac{K-1}{2K}} < m/2$. A (2.5) egyenlőtlenséget az

$$I_h = (m^{\frac{1}{2}+\frac{h-1}{2K}}, m^{\frac{1}{2}+\frac{h}{2K}}],$$

intervallumra alkalmazva (ahol h egy olyan pozitív egész szám, melyre $1 \le h \le K-1$ teljesül) azt kapjuk, hogy

$$\sum_{p \in I_h} \frac{1}{p} > \log \frac{K+h}{K+h-1} - \varepsilon.$$

Ha $p \in I_h$, akkor

$$\log^\lambda(m/p) \le \log^\lambda(m) \left(\frac{K-h+1}{2K} \right)^\lambda.$$

Behelyettesítve (2.3) utolsó sorának fő tagjába, elhagyva az egészrészeket és rendezve a következőket kapjuk:

$$\begin{aligned}
\sum_{\sqrt{m} < p < m/2} c \cdot \frac{m/p}{\log^\lambda(\lfloor m/p \rfloor)} &\ge cm \sum_{\sqrt{m} < p < m/2} \frac{1/p}{\log^\lambda(m/p)} \ge \\
&\ge \frac{cm}{\log^\lambda m} \sum_{h=1}^{K-1} \sum_{p \in I_h} \left(\frac{2K}{K-h+1} \right)^\lambda \cdot \frac{1}{p} \ge \\
&\ge \frac{cm}{\log^\lambda m} \sum_{h=1}^{K-1} \left(\frac{2K}{K-h+1} \right)^\lambda \log \frac{K+h}{K+h-1} - \\
&\qquad - \frac{cm}{\log^\lambda m} \cdot \varepsilon \sum_{h=1}^{K-1} \left(\frac{2K}{K-h+1} \right)^\lambda .
\end{aligned} \tag{2.6}$$

Most megmutatjuk, hogy létezik olyan K, melyre

$$S_K = \sum_{h=1}^{K-1} \left(\frac{2K}{K-h+1} \right)^{\lambda} \log \frac{K+h}{K+h-1} > 1$$

teljesül. Legyen

$$f_K(y) = \left(\frac{2}{y} \right)^{\lambda} K \cdot \log \left(1 + \frac{1}{K(2-y)} \right) \text{ és } f(y) = \left(\frac{2}{y} \right)^{\lambda} \cdot \frac{1}{2-y}.$$

Az f_K függvénysorozat f-hez konvergál. Legyen

$$S_K = \frac{f_K(\frac{1}{K}) + f_K(\frac{2}{K}) + \cdots + f_K(\frac{K}{K})}{K} - \frac{f_K(\frac{1}{K})}{K},$$

$$T_K = \frac{f(\frac{1}{K}) + f(\frac{2}{K}) + \cdots + f(\frac{K}{K})}{K}.$$

Mivel $1 > \lambda > \lambda_0$, ezért a T_k Riemann-összeg határértéke $\int_0^1 f > 1$. Mivel $f_K(\frac{1}{K})/K$ a 0-hoz tart, ezért $S_K - T_K$ határértéke szintén 0. Így rögzíthetünk egy olyan K számot, melyre $S_K > 1$. Válasszunk most egy olyan $\varepsilon > 0$ számot, melyre teljesül, hogy

$$\eta = \sum_{h=1}^{K-1} \left(\frac{2K}{K-h+1} \right)^{\lambda} \log \frac{K+h}{K+h-1} - 1 - \varepsilon \sum_{h=1}^{K-1} \left(\frac{2K}{K-h+1} \right)^{\lambda} > 0.$$

A (2.4) egyenlőtlenség szerint létezik olyan R, hogy ha $R < m$, akkor

$$\sum_{\sqrt{m}<p<m/2} c \cdot \frac{1}{\log^{\lambda}(\lfloor m/p \rfloor)} \leq \eta \cdot c \cdot \frac{m}{\log^{\lambda} m}.$$

A (2.3) és a (2.6) egyenlőtlenségek segítségével azt kapjuk, hogy

$$g_1(m) \geq c \cdot \frac{m}{\log^{\lambda} m}$$

teljesül. Mivel $c > 0$ értékét megválaszthatjuk úgy, hogy (2.2) teljesüljön $n \leq \max(2^{2K}, B^2(\varepsilon), R)$ esetén is, ezért ezzel a tételt igazoltuk.

□

2.2. $K = \{1, 2, \ldots, k\}$

Ebben az alfejezetben igazoljuk a 2.1. Sejtést.

2.3. Tétel. *Legyenek $k \leq n$ tetszőleges pozitív egész számok. Ekkor $|\underline{n} * \underline{k}| \geq n$.*

Bizonyítás. A bizonyításban több esetet különböztetünk meg aszerint, hogy k milyen nagyságrendű n-hez viszonyítva. A sejtés $k \leq 8$ esetén igaz ([32]).

1. eset: $9 \leq k \leq 1,34 \cdot \log n$

Megmutatjuk, hogy ebben az esetben az $\underline{n} \cdot \underline{k}$ szorzatban pontosan egyszer szereplő elemek száma is legalább n. A következő észrevételeket fogjuk használni:

2.4. Lemma. *Legyen $a \in (n/2, n]$ olyan pozitív egész szám, mely relatív prím minden k-nál nem nagyobb pozitív egész számhoz és legyen $b \in \underline{k}$ tetszőleges. Ekkor $ab \in 1(\underline{n}, \underline{k})$.*

Bizonyítás. Tegyük fel, hogy $a_1, a_2 \in \underline{n}$ és $b_1, b_2 \in \underline{k}$ számokra $a_1 b_1 = a_2 b_2$, valamint a_1 és b_1 teljesítik a lemma feltételeit. Mivel $a_1 | a_2 b_2$ és $(a_1, b_2) = 1$, ezért $a_1 | a_2$. Továbbá $a_1 > n/2$ miatt $2a_1 > n \geq a_2$, és így $a_1 = a_2$, amiből $b_1 = b_2$ is következik. $\square$

2.5. Lemma. *Ha $k \geq 14$, akkor* $\displaystyle\prod_{p \leq k} \left(1 - \frac{1}{p}\right) \geq \frac{0,5}{\log k}$.

Bizonyítás. Rosser és Schoenfeld [37] igazolták, hogy $k > 1$ esetén

$$\frac{e^{-\gamma}}{\log k}\left(1 - \frac{1}{\log^2 k}\right) \leq \prod_{p \leq k}\left(1 - \frac{1}{p}\right),$$

ahol γ az Euler-féle konstans. Ha $k > 21$, akkor a logaritmusfüggvény monotonitását és $e^{-\gamma} > 0,56$ becslést használva az igazolni kívánt egyenlőtlenséget kapjuk:

$$\frac{e^{-\gamma}}{\log k}\left(1 - \frac{1}{\log^2 k}\right) \geq \frac{0,56}{\log k}\left(1 - \frac{1}{\log^2 22}\right) > \frac{0,5}{\log k}.$$

A $14 \leq k \leq 21$ esetek igazolásához elég ellenőrizni az állítást, amikor $k = 14$, 17, vagy 19. Ezekre az értékekre a $(\log k) \cdot \displaystyle\prod_{p \leq k}\left(1 - \frac{1}{p}\right)$ kifejezés értéke kerekítve rendre $0,506$, $0,511$, illetve $0,503$, tehát az állítás valóban teljesül. $\square$

2.6. Állítás. *Ha* $9 \leq k \leq 1,34 \cdot \log n$, *akkor* $|1(\underline{n}, \underline{k})| \geq n$.

Bizonyítás. Megmutatjuk, hogy legalább n olyan szorzat van, amelyre teljesülnek a 2.4. Lemma feltételei. Ehhez szükségünk van azon $n/2$ és n közé eső egészek számának becslésére, melyek egyetlen k-nál nem nagyobb prímszámmal sem oszthatók. Ezek számát jelölje D. A szita-formula szerint:

$$D = n - \lfloor n/2 \rfloor + \\ + \sum_{h=1}^{r} (-1)^h \sum_{1 \leq i_1 < \ldots < i_h \leq r} \left(\left\lfloor \frac{n}{p_{i_1} \ldots p_{i_h}} \right\rfloor - \left\lfloor \frac{n/2}{p_{i_1} \ldots p_{i_h}} \right\rfloor \right), \quad (2.7)$$

ahol $\pi(k) = r$ és $p_1, \ldots, p_r$ a k-nál nem nagyobb prímszámok. Az $x - 1 < \lfloor x \rfloor \leq x$ becslést alkalmazva a jobb oldal mind a 2^{r+1} tagjára azt kapjuk, hogy

$$D \geq n - n/2 + \\ + \left\{ \sum_{h=1}^{r} (-1)^h \sum_{1 \leq i_1 < \ldots < i_h \leq r} \left(\frac{n}{p_{i_1} \ldots p_{i_h}} - \frac{n/2}{p_{i_1} \ldots p_{i_h}} \right) \right\} - 2^r = \\ = \frac{n}{2} \left\{ \prod_{p \leq k} \left(1 - \frac{1}{p} \right) \right\} - 2^r. \quad (2.8)$$

Ha $k \geq 14$, akkor a 2.5. Lemma alkalmazható, így

$$D \geq \frac{n}{2} \left\{ \prod_{p \leq k} \left(1 - \frac{1}{p} \right) \right\} - 2^r \geq \frac{0,25n}{\log k} - 2^r.$$

Mivel $k \leq 1,34 \log n$, ezért $k \geq 14$ esetén teljesül a következő becslés:

$$2^r = 2^{\pi(k)} \leq 2^{k/2} \leq \frac{1}{100 \log k} \cdot e^{\frac{k}{1,34}} \leq \frac{n}{100 \log k}.$$

Tehát $D \geq \dfrac{0,24n}{\log k}$. Tudjuk, hogy a 2.4. Lemma szerint $|1(\underline{n}, \underline{k})| \geq Dk$. Az $x/\log x$ függvény az $(1, \infty)$ intervallumon monoton növő, ezért

$$|1(\underline{n}, \underline{k})| \geq Dk \geq \frac{0,24k}{\log k} n \geq \frac{0,24 \cdot 14}{\log 14} n > n.$$

Ha $9 \le k \le 13$, akkor

$$|1(\underline{n}, \underline{k})| \ge Dk \ge \left(\frac{n}{2} \left\{ \prod_{p \le k} \left(1 - \frac{1}{p}\right) \right\} - 2^{\pi(k)} \right) k.$$

A feltétel szerint $n \ge e^{k/1,34}$ is teljesül. Ezekből $10 \le k \le 13$ esetén levezethető, hogy a jobb oldal nagyobb, mint n. Ha $k = 9$, akkor a jobb oldal nagyobb n-nél $n > 5040$ esetén. Számítógéppel ellenőrizhető, hogy az állítás $k = 9$ és $n \le 5040$ esetén is teljesül. Ezzel igazoltuk, hogy $|1(\underline{n}, \underline{k})| > n$.

$\square$

2. eset: $1,34 \cdot \log n \le k \le n - \dfrac{0,22 \cdot n}{\log n}$ és $n \ge 1410$

Legyen $k_1 = \max(k, n/7)$ és legyen $p \in (k_1, n]$ egy prímszám. Mivel $k < p$, ezért az $\underline{n} * \underline{k}$ halmaz p-vel osztható elemeinek halmaza nem más mint $\{p, 2p, \ldots, \lfloor n/p \rfloor p\} * \underline{k}$. Ennek a halmaznak ugyanannyi eleme van, mint az $\underline{\lfloor n/p \rfloor} * \underline{k}$ halmaznak. Mivel $\lfloor n/p \rfloor \le 6$, ezért $|\underline{\lfloor n/p \rfloor} * \underline{k}| \ge k$. Ha p és q olyan prímszámok, melyek nagyobbak $n/7$-nél, akkor $\underline{n} * \underline{k}$ egy eleme nem lehet egyszerre osztható p-vel és q-val is. Ezért $|\underline{n} * \underline{k}| \ge (\pi(n) - \pi(k_1))k$.

Először tegyük fel, hogy $k \le n/7$. Dusart [7] tétele szerint, ha $x \ge 17$, akkor

$$\frac{x}{\log x} \le \pi(x) \le \frac{x}{\log x}\left(1 + \frac{1,2762}{\log x}\right)$$

teljesül. Így $\pi(n) - \pi(n/7) \ge 0,749 \cdot \dfrac{n}{\log n}$, ha $n \ge 1410$. Mivel $1,34 \cdot \log n \le k$, ezért

$$|\underline{n} * \underline{k}| \ge 1,34 \cdot 0,749 \cdot n > n.$$

Most tegyük fel, hogy $n/7 < k \le n/2$. Mivel $\pi(n) - \pi(n/2) \ge 7$, ezért

$$|\underline{n} * \underline{k}| \ge (\pi(n) - \pi(k_1))k > 7 \cdot n/7 = n.$$

Végül, legyen $n/2 < k < n - \dfrac{0,22 \cdot n}{\log n}$. Ekkor a [7]-ben és [36]-ban szereplő becsléseket használva megmutatható, hogy legalább két prím esik k és n közé, ha $n > 90000$. Ellenőrizhető, hogy ez már minden $n > 1410$ esetén is teljesül. Tehát megmutattuk, hogy

$$|\underline{n} * \underline{k}| \ge (\pi(n) - \pi(k))k \ge 2(n/2) = n.$$

Azzal az esettel folytatjuk, amikor k „nagy", azaz $n - \frac{0,4 \cdot n}{\log n + 1,02} \leq k$ teljesül. Könnyű számolás mutatja, hogy ha $n \geq 4$, akkor $n - \frac{0,4 \cdot n}{\log n + 1,02} \leq n - \frac{0,22 \cdot n}{\log n}$.

3. eset: $n - \dfrac{0,4 \cdot n}{\log n + 1,02} \leq k \leq n$ és $n > 5000$

Ha $k = n$, akkor $\underline{k} \cdot \underline{n} = \{1, \ldots, n\} \cdot \{1, \ldots, n\}$. Az ab szorzatot párba állíthatjuk a ba szorzattal, ha $a \neq b$. Ily módon csak az $a \cdot a$ alakú szorzatok maradnak pár nélkül, ezért $\underline{n} * \underline{k} = \{1^2, 2^2, \ldots, n^2\}$, és így

$$|\underline{n} * \underline{k}| = n.$$

Tegyük fel, hogy $k < n$. Tekintsük a következő átalakításokat:

$$\begin{aligned}|\underline{n} * \underline{k}| &= |(\underline{k} * \underline{k}) \Delta ((\underline{n} \setminus \underline{k}) * \underline{k})| = \\ &= |\underline{k} * \underline{k}| + |(\underline{n} \setminus \underline{k}) * \underline{k}| - 2|(\underline{k} * \underline{k}) \cap ((\underline{n} \setminus \underline{k}) * \underline{k})|. \end{aligned} \tag{2.9}$$

A (2.9) egyenlet jobb oldalának első tagjára teljesül, hogy

$$|\underline{k} * \underline{k}| = |\{1^2, 2^2, \ldots, k^2\}| = k. \tag{2.10}$$

2.7. Lemma. *A (2.9) egyenlet jobb oldalának második tagjára teljesül, hogy*

$$|(\underline{n} \setminus \underline{k}) * \underline{k}| \geq 2k - n. \tag{2.11}$$

Bizonyítás. A következő észrevételt fogjuk használni: ha

$$i \leq \frac{k}{n-k} \quad \text{és} \quad k + 1 \leq j \leq n,$$

akkor $ij \in 1(\underline{n} \setminus \underline{k}, \underline{k})$, vagyis $ij \in (\underline{n} \setminus \underline{k}) * \underline{k}$. Tegyük fel, hogy $ij = i'j'$, ahol $1 \leq i' \leq k$ és $k + 1 \leq j' \leq n$. Ha $i = i'$, akkor $j = j'$. Ha $i' < i$, akkor $1 \leq i' \leq \dfrac{k}{n-k}$ és $k + 1 \leq j' \leq n$. Ekkor az (i, j) és (i', j') párok szerepét megcserélve feltehető, hogy $i < i'$. Mivel $ij = i'j'$, ezért $\dfrac{i}{i'} = \dfrac{j'}{j}$ és

$$\frac{i}{i'} \leq \frac{i}{i+1} \leq \frac{\frac{k}{n-k}}{\frac{k}{n-k} + 1} = \frac{k}{n} < \frac{k+1}{n} \leq \frac{j'}{j},$$

ami ellentmondás. Így $(\underline{n} \setminus \underline{k}) * \underline{k}$ elemszámára azt kaptuk, hogy

$$|(\underline{n} \setminus \underline{k}) * \underline{k}| \geq \left\lfloor \frac{k}{n-k} \right\rfloor (n-k) \geq$$
$$\geq \left(\frac{k}{n-k} - 1 \right) (n-k) = k - (n-k) = 2k - n. \quad (2.12)$$

□

Most (2.9) jobb oldalának harmadik tagját fogjuk vizsgálni.

2.8. Lemma. *A (2.9) egyenlet jobb oldalának harmadik tagjára*

$$|(\underline{k} * \underline{k}) \cap ((\underline{n} \setminus \underline{k}) * \underline{k})| \leq 0,431 \cdot k. \quad (2.13)$$

teljesül.

Bizonyítás. Elég igazolni, hogy az 1^2, 2^2, ..., k^2 számok közül legfeljebb $0,431k$-nak van olyan osztója, mely a $[k+1, n]$ intervallumba esik. Legyen $k+1 \leq m \leq n$ és $m = a_m b_m^2$, ahol b_m^2 az m szám legnagyobb négyzetszám osztója. Mivel a_m négyzetmentes, ezért $m|i^2$ pontosan akkor teljesül, ha $a_m b_m | i$. Így az $\{1^2, 2^2, \ldots, k^2\}$ halmazba eső $[k+1, n]$-beli osztóval rendelkező számok számára a következő felső becslést adhatjuk:

$$\sum_{m=k+1}^{n} \left\lfloor \frac{k}{a_m b_m} \right\rfloor \leq \sum_{m=k+1}^{n} \frac{k}{a_m b_m} = k \sum_{m=k+1}^{n} \frac{b_m}{m}.$$

Az m számot $m = a_m b_m^2$ alakban (ahol a_m négyzetmentes) felírva, $j = b_m \leq \sqrt{m}$ szerint összegezve, és a becslést folytatva:

$$k \sum_{m=k+1}^{n} \frac{b_m}{m} = k \sum_{j=1}^{\lfloor \sqrt{n} \rfloor} \sum_{\substack{j^2|m,\\ k+1 \leq m \leq n,\\ |\mu(m/j^2)|=1}} \frac{j}{m} \leq k \sum_{j=1}^{\lfloor \sqrt{n} \rfloor} j \sum_{\substack{j^2|m,\\ k+1 \leq m \leq n}} \frac{1}{m}.$$

A kapott felső becslést jelölje S. Legyen

$$S_1 := \sum_{j=1}^{\lfloor \sqrt{n}/2 \rfloor} j \sum_{\substack{j^2|m,\\ k+1 \leq m \leq n}} \frac{1}{m} \quad \text{és} \quad S_2 := \sum_{j=\lfloor \sqrt{n}/2 \rfloor + 1}^{\lfloor \sqrt{n} \rfloor} j \sum_{\substack{j^2|m,\\ k+1 \leq m \leq n}} \frac{1}{m}.$$

Ekkor $S = k(S_1 + S_2)$. Először S_1-re adunk felső becslést.

2.9. Lemma.
$$S_1 \le \left(\frac{\log n}{2} + 0,31\right)(\log n - \log k) + \frac{n + 2\sqrt{n}}{8k}. \tag{2.14}$$

Bizonyítás. Legyen $r_j = \left\lceil \frac{k+1}{j^2} \right\rceil$ és $s_j = \left\lfloor \frac{n}{j^2} \right\rfloor$. Ekkor
$$S_1 = \sum_{j=1}^{\lfloor\sqrt{n}/2\rfloor} j \sum_{l=r_j}^{s_j} \frac{1}{lj^2} = \sum_{j=1}^{\lfloor\sqrt{n}/2\rfloor} \frac{1}{j} \sum_{l=r_j}^{s_j} \frac{1}{l}. \tag{2.15}$$

Az $\frac{1}{x}$ függvény nemnegatív és monoton csökkenő a $(0,\infty)$ intervallumon, ezért a belső összeget a következő módon becsülhetjük:
$$\sum_{l=r_j}^{s_j} \frac{1}{l} \le \int_{r_j}^{s_j} 1/x + \frac{1}{r_j} = \log s_j - \log r_j + \frac{1}{r_j}.$$

Mivel $\frac{k}{j^2} \le r_j$ és $s_j \le \frac{n}{j^2}$, ezért
$$\log s_j - \log r_j = \log \frac{s_j}{r_j} \le \log \frac{n/j^2}{k/j^2} = \log n - \log k.$$

Ezt (2.15)-be helyettesítve azt kapjuk, hogy:
$$S_1 \le \sum_{j=1}^{\lfloor\sqrt{n}/2\rfloor} \frac{1}{j}\left(\log s_j - \log r_j + \frac{1}{r_j}\right) \le$$
$$\le \sum_{j=1}^{\lfloor\sqrt{n}/2\rfloor} \frac{1}{j}\left(\log n - \log k + \frac{j^2}{k}\right). \tag{2.16}$$

Mivel
$$\sum_{j=1}^{\lfloor\sqrt{n}/2\rfloor} \frac{1}{j} \le \log\lfloor\sqrt{n}/2\rfloor + 1 \le \frac{\log n}{2} - \log 2 + 1 \le \frac{\log n}{2} + 0,31 \tag{2.17}$$

és
$$\sum_{j=1}^{\lfloor\sqrt{n}/2\rfloor} j = \frac{\lfloor\sqrt{n}/2\rfloor \cdot (\lfloor\sqrt{n}/2\rfloor + 1)}{2} \le \frac{n + 2\sqrt{n}}{8}, \tag{2.18}$$

ezért a (2.16), (2.17), (2.18) egyenlőtlenségekből (2.14)-et kapjuk. $\square$

Most S_2-re adunk felső becslést.

2.10. Lemma.

$$S_2 \le \left(1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}}\right) \cdot \frac{n-k}{2\sqrt{k}} \cdot \frac{\sqrt{n}}{k} + \frac{3\sqrt{n}}{k} < \\ < 1,15 \cdot \frac{(n-k)\sqrt{n}}{k^{3/2}} + \frac{3\sqrt{n}}{k}. \quad (2.19)$$

Bizonyítás. Az

$$S_2 = \sum_{j=\lfloor\sqrt{n}/2\rfloor+1}^{\lfloor\sqrt{n}\rfloor} \sum_{\substack{j^2|m, \\ k+1\le m\le n}} \frac{j}{m} \quad (2.20)$$

összeget szeretnénk becsülni. A (2.20) egyenletben minden j-re

$$n \ge j^2 \ge (\lfloor\sqrt{n}/2\rfloor + 1)^2 > \frac{n}{4}.$$

Ezért $m = j^2$, $2j^2$ vagy $3j^2$. Mivel $k < m \le n$, ezért $m = ij^2$ $(i = 1, 2, 3)$ esetén

$$\sqrt{\frac{k}{i}} < j \le \sqrt{\frac{n}{i}} \quad \text{és} \quad \frac{j}{m} \le \frac{\sqrt{n}}{k}.$$

Ha i értékét rögzítjük, akkor az olyan j számok száma, melyekre $m = ij^2$ teljesül felülről becsülhető a következővel:

$$\left\lceil \frac{\sqrt{n}-\sqrt{k}}{\sqrt{i}} \right\rceil = \left\lceil \frac{1}{\sqrt{i}} \cdot \frac{n-k}{\sqrt{n}+\sqrt{k}} \right\rceil \le \frac{1}{\sqrt{i}} \cdot \frac{n-k}{2\sqrt{k}} + 1,$$

ezért

$$S_2 \le \left(1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}}\right) \cdot \frac{n-k}{2\sqrt{k}} \cdot \frac{\sqrt{n}}{k} + \frac{3\sqrt{n}}{k} < 1,15 \cdot \frac{(n-k)\sqrt{n}}{k^{3/2}} + \frac{3\sqrt{n}}{k},$$

és mi éppen ezt akartuk igazolni. □

Az eredményeket összefoglalva, (2.14) és (2.19) egyenletekből a következő becslést kapjuk:

$$\frac{S}{k} = S_1 + S_2 \leq \left(\frac{\log n}{2} + 0,31\right)(\log n - \log k) + \\ + \frac{n + 2\sqrt{n}}{8k} + 1,15 \cdot \frac{(n-k)\sqrt{n}}{k^{3/2}} + \frac{3\sqrt{n}}{k}. \quad (2.21)$$

A feltevésünk szerint $n - \frac{0,4 \cdot n}{\log n + 1,02} \leq k$ és $n \geq 5000$. Az $e^{-x} < \frac{1}{1+x}$ egyenlőtlenséget felhasználva azt kapjuk, hogy

$$ne^{-\frac{0,2}{\frac{\log n}{2}+0,31}} < n \cdot \frac{1}{1 + \frac{0,2}{\frac{\log n}{2}+0,31}} = n - \frac{0,4 \cdot n}{\log n + 1,02} \leq k.$$

Mivel $n > 5000$, ezért $\frac{k}{n} > 0,958$. Ezekből az egyenlőtlenségekből könnyű számolással a következő becslések vezethetők le:

$$\left(\frac{\log n}{2} + 0,31\right)(\log n - \log k) < 0,2, \quad (2.22)$$

$$\frac{n + 2\sqrt{n}}{8k} < 0,135, \quad (2.23)$$

$$1,15 \cdot \frac{(n-k)\sqrt{n}}{k^{3/2}} + \frac{3\sqrt{n}}{k} < 0,096. \quad (2.24)$$

A (2.22), (2.23) és (2.24) egyenlőtlenségeket összeadva és (2.21)-et használva a kívánt becslést kapjuk:

$$S \leq k\,(0,2 + 0,135 + 0,096) = 0,431 \cdot k.$$

Ekkor a (2.10), (2.11) és (2.13) egyenlőtlenségekből $k/n > 0,958$ esetén azt kapjuk, hogy

$$|\underline{k} * \underline{n}| \geq k + 2k - n - 2S \geq 2,138 \cdot k - n > n,$$

ezzel az állítást a 3. esetben is igazoltuk. □

Beláttuk az állítást az összes olyan n, k párra, ahol $n \geq 5000$. A $k \leq n \leq 5000$ esetek számítógéppel ellenőrizhetők.

□

3. fejezet

Ramsey-típusú és sűrűségi tételek egyenletek megoldhatóságáról $\mathbb{N}$-ben

3.1. Az $ab = c$ egyenlet

Ebben a fejezetben egyenletek $\mathbb{N}$-beli megoldhatóságára vonatkozó Ramsey-típusú és sűrűségi tételeket igazolunk.

2009-ben megjelent cikkükben Hajdu, Schinzel és Skałba [19] azt vizsgálták, hogy milyen sűrű lehet a pozitív egész számok egy olyan részhalmaza, melyben az $ab = c$ egyenletnek nincsen megoldása. Igazolták, hogy egy ilyen tulajdonságú részhalmaz felső sűrűsége tetszőlegesen közel lehet 1-hez. Később azonban Pomerance és Schinzel [33] bebizonyították, hogy ha a négyzetmentes számok halmazát 2 színnel színezzük, akkor az $ab = c$ egyenletnek biztosan van monokromatikus megoldása. Cikkükben az alábbi problémát vetették fel:

3.1. Probléma. Igaz, hogy az 1-nél nagyobb négyzetmentes számok tetszőleges r-színezése esetén létezik az $ab = c$ egyenletnek monokromatikus megoldása?

Pomerance és Schinzel azért szorítkoztak négyzetmentes számokra, mert Schur tételéből könnyen következik, hogy ha $\mathbb{N}$-et r színnel színezzük, akkor az $ab = c$ egyenletnek mindig létezik monokromatikus megoldása, már a 2-hatványok körében is:

3.2. Állítás. *A 2-hatványok tetszőleges r-színezése esetén létezik monokromatikus megoldása az $ab = c$ egyenletnek.*

Bizonyítás. Tekintsük a 2-hatványok egy tetszőleges r-színezését. Definiáljuk $\mathbb{N}$ egy r-színezését a következő módon: legyen $x \in \mathbb{N}$ színe 2^x színe. Schur tétele [41] szerint az $x+y = z$ egyenletnek létezik monokromatikus megoldása $\mathbb{N}$-ben. Ekkor az $ab = c$ egyenletnek szintén létezik (az eredeti színezésre nézve) monokromatikus megoldása a 2-hatványok körében, nevezetesen: $a = 2^x, b = 2^y, c = 2^z$. □

Ebben a fejezetben a problémát teljes általánosságban megoldjuk. Az eredményt általánosabb egyenletekre kiterjesztve a 3.5. Tételben igazoljuk, hogy tetszőleges $k \geq 2, l, r$ pozitív egész számok esetén létezik az

$$a_1 a_2 \dots a_k = b_1 b_2 \dots b_l$$

egyenletnek is monokromatikus megoldása a négyzetmentes számok tetszőleges r-színezése esetén.

A fejezet során sűrűségi tételnek nevezünk egy olyan típusú eredményt, mely azt mondja ki, hogy ha kiválasztjuk a megadott halmaznak egy „kellően nagy" részhalmazát, akkor ebben megoldható egy rögzített egyenlet. Ramsey-típusú eredményről pedig akkor beszélünk, ha a megadott halmaz elemeit r színnel színezve az egyenletünknek létezik monokromatikus megoldása. A sűrűségi tételből mindig következik Ramsey-típusú tétel is, hiszen a legnagyobb színosztályba tartozó elemek egy „sűrű" részhalmazt alkotnak. Ugyanakkor Ramsey-típusú tétel akkor is teljesülhet, ha a sűrűségi tétel nem igaz, vagy sokkal nehezebben igazolható. Ismert példa van der Waerden [43], illetve Szemerédi [42] számtani sorozatokra vonatkozó tétele, ahol mindkét típusú tétel igaz, azonban a sűrűségi tételt csak 58 évvel a Ramsey-típusú eredmény bizonyítása után sikerült igazolni.

A fejezetben a bizonyítások során szükségünk lesz néhány ismert tételre. Ilyen például Ramsey tételének következő alakja ([14], [24]):

Ramsey tétele. Legyenek r, t és n pozitív egész számok. Ekkor létezik olyan d pozitív egész szám, melyre teljesül a következő. Ha S egy olyan halmaz, melynek elemszáma $|S| > d$, és adott az S halmaz legfeljebb t elemű részhalmazainak egy tetszőleges r-színezése, akkor S-nek van olyan n elemű H részhalmaza, hogy H bármely két egyforma méretű, legfeljebb t elemű részhalmaza egyforma színű, azaz, minden $H_1, H_2 \subseteq H$, $|H_1| = |H_2| \leq t$ esetén H_1 és H_2 egyforma színűek.

Ramsey tétele szerint minden n esetén létezik olyan d, hogy ha $|S| > d$, akkor létezik olyan $H \subseteq S$, $|H| = n$, hogy H minden 1 elemű részhalmaza egyforma színű, minden 2 elemű részhalmaza egyforma színű, és így tovább, H minden t elemű részhalmaza egyforma színű. Az ilyen tulajdonságú d számot Ramsey-számnak hívják.

Rado tételének következő alakját szintén használni fogjuk ([24], [34]):

Rado tétele. Legyen $v \geq 2$ pozitív egész szám. Legyenek a $c_i \in \mathbb{Z} \setminus \{0\}$ (ahol $1 \leq i \leq v$) számok olyan konstansok, melyekre létezik olyan nemüres $D \subseteq \{c_i : 1 \leq i \leq v\}$ halmaz, hogy $\sum\limits_{d \in D} d = 0$. Ha léteznek olyan páronként különböző (nem feltétlenül pozitív) egész $y_1, \dots, y_v$ számok, hogy $\sum c_i y_i = 0$, akkor minden r pozitív egész szám esetén létezik olyan t, hogy az $\{1, 2, \dots, t\}$ halmaz tetszőleges r-színezése esetén a

$$c_1 x_1 + \cdots + c_v x_v = 0 \tag{3.1}$$

egyenletnek van páronként különböző egész számokból álló monokromatikus megoldása $\{1, 2, \dots, t\}$-ben.

A fejezet eredményei [26]-ban olvashatók.

3.2. Az $a_1 a_2 \dots a_k = b_1 b_2 \dots b_l$ egyenlet

Hajdu, Schinzel és Skałba már említett eredménye szerint az $ab = c$ egyenlet esetében nincsen sűrűségi tétel. A következő példa megmutatja, hogy ha $k \neq l$, akkor az általánosabb

$$a_1 a_2 \dots a_k = b_1 b_2 \dots b_l \tag{3.2}$$

egyenlet esetében sem teljesül sűrűségi tétel.

3.3. Példa. Legyen

$$\mathcal{A}_n = \{4i + 2 : 0 \leq i,\ 4i + 2 \leq n\}.$$

Ha

$$a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_l \in \mathcal{A}_n,$$

akkor az $a_1 a_2 \dots a_k$ szám prímtényezős felbontásában a 2 kitevője k, míg $b_1 b_2 \dots b_l$ számában l. Így a (3.2) egyenlet nem oldható meg $\mathcal{A}_n$-ben, hiszen $k \neq l$. Az $\mathcal{A}_n$ halmaz mérete

$$|\mathcal{A}_n| = \frac{1}{4} \cdot n + O(1).$$

Más a helyzet azonban, ha $k = l$. Ekkor

$$a_1 = \cdots = a_k = b_1 = \cdots = b_k$$

mindig megoldása a (3.2) egyenletnek. Az ilyen triviális megoldások elkerülése végett azt mondjuk, hogy az

$$a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_l$$

számok egy primitív megoldását alkotják a (3.2) egyenletnek, ha ők páronként különbözők. Mostantól csak az egyenletek primitív megoldásait keressük, hiszen nem primitív megoldások létezése általában könnyen igazolható. Szemben a $k \neq l$ esettel, $k = l$ esetén már akkor is igazolható sűrűségi tétel, ha csak a primitív megoldásokra szorítkozunk.

3.4. Állítás. *Legyen $2 \leq k \in \mathbb{N}$ tetszőleges egész szám. Ekkor minden $\varepsilon > 0$-hoz létezik olyan $N = N(\varepsilon)$, hogy ha $n \geq N$, akkor $\mathcal{A} \subseteq \{1, 2, \ldots, n\}$ és $|\mathcal{A}| \geq \varepsilon n$ esetén az $a_1 a_2 \ldots a_k = b_1 b_2 \ldots b_k$ egyenletnek van primitív megoldása $\mathcal{A}$-ban.*

Bizonyítás. Az állítást k szerinti teljes indukcióval bizonyítjuk. Először legyen $k = 2$ és $\varepsilon > 0$ tetszőleges. Az N korlátot később fogjuk meghatározni. Legyen $\mathcal{A} \subseteq \{1, 2, \ldots, n\}$, ahol $n \geq N$ és $|\mathcal{A}| > \varepsilon n$. Erdős [10] igazolta, hogy az $1, 2, \ldots, n$ számokból képzett „szorzótábla" csak $o(n^2)$ féle szorzatot tartalmaz, azaz $|\{a \cdot b \mid a, b \in \{1, 2, \ldots, n\}\}| = o(n^2)$. Mivel $\mathcal{A} \subseteq \{1, 2, \ldots, n\}$, ezért az $\mathcal{A} \cdot \mathcal{A} = \{c_1 c_2 \mid c_1, c_2 \in \mathcal{A}\}$ halmaz elemeinek száma legfeljebb $o(n^2)$. Viszont $\binom{|\mathcal{A}|}{2} = \frac{\varepsilon^2}{2} \cdot n^2 + o(n^2)$ féle olyan c_1, c_2 pár létezik, melyre $c_1, c_2 \in \mathcal{A}$ és $c_1 \neq c_2$ feltételek teljesülnek. Válasszuk meg N értékét úgy, hogy $N < n$ esetén tetszőleges legalább εn elemű $\mathcal{A} \subseteq \{1, 2, \ldots, n\}$ halmazra $\binom{|\mathcal{A}|}{2} > |\mathcal{A} \cdot \mathcal{A}|$ legyen. Ekkor van $\mathcal{A} \cdot \mathcal{A}$-ban olyan szám, amely legalább kétféleképpen felírható az $\mathcal{A}$ halmaz két különböző elemének szorzataként, vagyis vannak olyan $a_1, a_2, b_1, b_2 \in \mathcal{A}$ különböző elemek, amelyekre $a_1 a_2 = b_1 b_2$. Ily módon egy primitív megoldást kaptunk $k = 2$-re.

Legyen most $k = 3$. Jelölje $N_2(x)$ az $x = ab$ egyenlet különböző $\mathcal{A}$-beli elemekből álló megoldásainak számát:

$$N_2(x) = |\{(a, b) \mid x = ab, a < b, a, b \in \mathcal{A}\}|.$$

Tegyük fel, hogy vannak olyan páronként különböző $a, b, c \in \mathcal{A}$ számok, melyekre $N_2(ab) \geq 5$ és $N_2(ac) \geq 3$ is teljesül. Megmutatjuk, hogy ekkor az

$a_1a_2a_3 = b_1b_2b_3$ egyenletnek van primitív megoldása $\mathcal{A}$-ban. Mivel $N_2(ac) \geq 3$, ezért az ac szám felírható az $\mathcal{A} \setminus \{a, b, c\}$ halmaz két különböző elemének szorzataként. Legyen ez a két elem a' és c'. Mivel $N_2(ab) \geq 5$, ezért az ab szám felírható az $\mathcal{A}\setminus\{a', b, c', c\}$ halmaz két különböző elemének szorzataként. Legyen ez a két elem a'' és b''. Ekkor a'', b'', a', b, c', c különböző egész számok, és $a'bc' = abc = a''b''c$, azaz kaptunk egy primitív megoldás $\mathcal{A}$-ban.

Tegyük fel, hogy az $a_1a_2a_3 = b_1b_2b_3$ egyenletnek nincsen primitív megoldása $\mathcal{A}$-ban. Ekkor a fentiek miatt tetszőleges $a \in \mathcal{A}$ esetén legfeljebb egy olyan $b \in \mathcal{A}$ létezik, hogy $N_2(ab) \geq 5$. Tehát minden $a \in \mathcal{A}$-hoz legalább $|\mathcal{A}| - 2$ olyan $b \in \mathcal{A}$ létezik, amelyre $N_2(ab) \leq 4$. Ezért $|\mathcal{A} \cdot \mathcal{A}| > \frac{1}{4} \cdot \frac{|\mathcal{A}|(|\mathcal{A}|-2)}{2}$. A $k = 2$ esethez hasonlóan N megfelelő választása mellett ez ellentmond az $|\mathcal{A} \cdot \mathcal{A}| = o(n^2)$ összefüggésnek.

Most tegyük fel, hogy $4 \leq k \in \mathbb{N}$ és az állítást már igazoltuk $(k-2)$-re. Legyen $\varepsilon > 0$ tetszőleges. Az indukciós feltevés miatt létezik olyan N, hogy $N < n$ esetén minden olyan $\mathcal{B} \subseteq \{1, 2, \ldots, n\}$ halmazban, melynek legalább $\frac{\varepsilon}{3} \cdot n$ eleme van, az $a_1a_2 \ldots a_{k-2} = b_1b_2 \ldots b_{k-2}$ és $a_{k-1}a_k = b_{k-1}b_k$ egyenleteknek van primitív megoldása. Legyen $\mathcal{A} \subseteq \{1, 2, \ldots, n\}$ olyan halmaz, melynek legalább εn eleme van. Ha $n \geq 6/\varepsilon$, akkor $\mathcal{A}$ felosztható két diszjunkt részre, $\mathcal{A}_1$-re és $\mathcal{A}_2$-re, úgy, hogy mindkét rész elemszáma legalább $\frac{\varepsilon}{3} \cdot n$. Ha $n \geq N$, akkor az $a_1a_2 \ldots a_{k-2} = b_1b_2 \ldots b_{k-2}$ egyenletnek van primitív megoldása $\mathcal{A}_1$-ben és az $a_{k-1}a_k = b_{k-1}b_k$ egyenletnek van primitív megoldása $\mathcal{A}_2$-ben. Így az $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k$ számok az $a_1a_2 \ldots a_k = b_1b_2 \ldots b_k$ egyenlet egy primitív megoldását alkotják $\mathcal{A}$-ban.

$\square$

Most megmutatjuk, hogy az 1-nél nagyobb négyzetmentes számok tetszőleges r-színezése esetén van primitív megoldása a (3.2) egyenletnek, ha $k \geq 2$.

3.5. Tétel. *Legyenek $k \geq 2, l, r \in \mathbb{N}$ tetszőleges pozitív egész számok. Ekkor az 1-nél nagyobb négyzetmentes számok tetszőleges r-színezése esetén az*

$$a_1a_2 \ldots a_k = b_1b_2 \ldots b_l$$

egyenletnek létezik primitív monokromatikus megoldása.

Bizonyítás. A négyzetmentes számok kölcsönösen egyértelműen megfeleltethetők a prímszámok véges részhalmazainak: minden négyzetmentes számhoz rendeljük hozzá a prímosztóinak halmazát. Két négyzetmentes szám szorzata pontosan akkor lesz négyzetmentes, ha ezek a halmazok diszjunktak. Ebben az esetben a szorzathoz a két halmaz uniója tartozik.

Tegyük fel, hogy adott a négyzetmentes számok egy tetszőleges r-színezése. Definiáljuk a prímszámok véges részhalmazainak egy r-színezését a következő módon: egy részhalmaz színe legyen a benne szereplő elemek szorzatának színe. Tegyük fel, hogy az $A_1, \ldots, A_k, B_1, \ldots, B_l$ nemüres, véges, prímszámokból álló halmazokra teljesülnek az alábbi feltételek:

(i) $\cup A_i = \cup B_j$, valamint

(ii) $A_1, \ldots, A_k, B_1, \ldots, B_l$ egyforma színűek, és

(iii) $A_1, \ldots, A_k, B_1, \ldots, B_l$ páronként különbözők.

Ekkor az

$$a_i = \prod_{p \in A_i} p \text{ (ahol } 1 \leq i \leq k) \text{ és } b_j = \prod_{p \in B_j} p \text{ (ahol } 1 \leq j \leq l)$$

számok a (3.2) egyenlet egy primitív monokromatikus megoldását alkotják. Most belátjuk, hogy léteznek olyan, az (i)-(iii) feltételeket kielégítő $A_1, \ldots, A_k, B_1, \ldots, B_l$ halmazok, amelyekre (iii) helyett teljesül a következő erősebb feltétel is:

(iii') $|A_1| = \alpha_1, \ldots, |A_k| = \alpha_k, |B_1| = \beta_1, \ldots, |B_l| = \beta_l$ páronként különbözők.

A halmazok elemszámára szükségszerűen fennálló

$$\alpha_1 + \cdots + \alpha_k = \beta_1 + \cdots + \beta_l \tag{3.3}$$

egyenlet ekvivalens az

$$\alpha_1 + \cdots + \alpha_k - \beta_1 - \cdots - \beta_l = 0$$

egyenlettel. A kapott egyenletre alkalmazható Rado tétele a

$$v = k + l,$$

$$c_i = 1 \text{ (ha } 1 \leq i \leq k), c_i = -1 \text{ (ha } k < i \leq v)$$

választással, ugyanis az

$$y_i = i \text{ (ha } 1 \leq i \leq k), \ y_i = -i \text{ (ha } k < i < v) \text{ és } y_v = \frac{(v-1)v}{2}$$

számok a (3.1) egyenlet páronként különböző egész számokból álló megoldását adják. Válasszuk meg t-t úgy, hogy az $\{1, 2, \ldots, t\}$ halmaz minden r-színezése esetén legyen monokromatikus megoldása a (3.3) egyenletnek $\{1, 2, \ldots, t\}$-ben. Alkalmazzuk Ramsey tételét ezzel a t-vel és $n = t \max(k, l)$-lel a prímszámok részhalmazainak fent definiált színezésére. A tétel szerint van olyan d, hogy az első d prímszámból álló halmaz részhalmazainak tetszőleges r-színezése esetén van a prímeknek olyan H részhalmaza, hogy $|H| = n$, és minden $j \leq t$ esetén a H halmaz j elemű részhalmazai egyforma színűek. Színezzük az $\{1, 2, \ldots, t\}$ halmaz elemeit r színnel a következő módon: ha $1 \leq i \leq t$, akkor legyen i színe a H halmaz i elemű részhalmazainak (közös) színe. Rado tétele szerint (3.3) egyenletnek van monokromatikus megoldása. Legyen

$$m = \alpha_1 + \cdots + \alpha_k = \beta_1 + \cdots + \beta_l,$$

ahol

$$\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_l$$

páronként különböző, t-nél nem nagyobb pozitív egész számok. Vegyük az első m darab H-beli prímből álló halmaznak egy olyan $A_1, \ldots, A_k$ partícióját, melyre $|A_i| = \alpha_i$ (ha $1 \leq i \leq k$), valamint egy olyan $B_1, \ldots, B_l$ partícióját, melyre $|B_j| = \beta_j$ (ha $1 \leq j \leq l$). Ezek a halmazok kielégítik az (i), (ii), (iii') feltételeket, így az állítást igazoltuk.

$\square$

4. fejezet

Ramsey-típusú és sűrűségi tételek egyenletek megoldhatóságáról $\mathbb{Z}_m$-ben

4.1. Szorzatok és összegek $\mathbb{Z}_m$-ben

Ebben a fejezetben $\mathbb{Z}_m$-beli sűrűségi és Ramsey-típusú tételeket vizsgálunk. Sárközy [39], [40] bizonyította, hogy ha $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ „nagy" részhalmazai $\mathbb{Z}_p$-nek, akkor az

$$a + b = cd \tag{4.1}$$

és az

$$ab + 1 = cd \tag{4.2}$$

egyenletnek is létezik olyan megoldása, melyre teljesül, hogy

$$a \in \mathcal{A}, b \in \mathcal{B}, c \in \mathcal{C}, d \in \mathcal{D}.$$

Gyarmati és Sárközy [17] a (4.1) és (4.2) egyenletek megoldhatóságáról szóló eredményeket kiterjesztették véges testekre. Számos cikkben vizsgálják (4.1)-hez és (4.2)-höz hasonló egyenletek megoldhatóságát véges testek, speciálisan $\mathbb{Z}_p$ felett. (Például: [15], [16].) Természetesen adódik az egyenletek megoldhatóságának vizsgálata $\mathbb{Z}_m$-ben is ([33]). A [6] és [17] cikkekben Csikvári, Gyarmati és Sárközy megemlítik, hogy tetszőleges m egész szám esetén az (4.1) és (4.2) egyenletek esetén nem teljesül sűrűségi tétel $\mathbb{Z}_m$-ben. Megkérdezik, hogy igazolható-e Ramsey-típusú eredmény, azaz igaz-e, hogy

$\mathbb{Z}_m$ tetszőleges r-színezése esetén van monokromatikus megoldása (4.1)-nek (illetve (4.2)-nek), ha r, a színek száma, rögzített és m elegendően nagy: $m > N(r)$?

4.1. Probléma. Létezik-e Ramsey-típusú eredmény (4.1), illetve (4.2) egyenlet megoldhatóságáról $\mathbb{Z}_m$-ben?

Hindman [21] megmutatta, hogy ha az $\mathbb{N}$ feletti megoldhatóságot vizsgáljuk, akkor létezik Ramsey-típusú tétel a (4.1) egyenlet esetén. Valójában a következő, ennél erősebb állítást bizonyította: $\mathbb{N}$ minden r-színezése esetén létezik az $a_1 + \cdots + a_n = b_1 \dots b_n$ egyenletnek olyan megoldása is, ahol nem csak az $a_1, \dots, a_n, b_1, \dots, b_n$ számok, hanem a $\sum\limits_{i \in I} a_i$ (ahol $\emptyset \neq I \subseteq \{1, \dots, n\}$) összegek és $\prod\limits_{j \in J} b_j$ (ahol $\emptyset \neq J \subseteq \{1, \dots, n\}$) szorzatok is páronként különbözők (kivéve $\sum\limits_{i=1}^{n} a_i$ és $\prod\limits_{j=1}^{n} b_j$), valamint ezek az összegek és szorzatok mind egyforma színűek.

Ebben a fejezetben a 4.1. Problémát vizsgáljuk $\mathbb{Z}_m$-ben. Először kizárjuk a (4.1) egyenlet triviális monokromatikus megoldásait, mint például $0 + 0 = 0 \cdot 0$ vagy $2 + 2 = 2 \cdot 2$. Azokat a megoldásokat fogjuk triviális (monokromatikus) megoldásnak nevezni, ahol $a = b = c = d$ teljesül. A második alfejezet 4.4. Tételében igazoljuk, hogy (4.1)-nek létezik nemtriviális monokromatikus megoldása is. A harmadik alfejezetben pedig ellenpéldát mutatunk a 4.1. Problémára a (4.2) egyenlet esetén. Azaz végtelen sok m-re megadjuk $\mathbb{Z}_m$ olyan r-színezését, melynél a (4.2) egyenletnek nincsen monokromatikus megoldása. Ebből az ellenpéldából látható, hogy $m > N(r)$ helyett a $p(m) > N(r)$ feltétel szükséges (ahol $p(m)$ az m szám legkisebb prímosztóját jelöli), különben nem igaz Ramsey-típusú eredmény. A 4.8. Következményben igazoljuk, hogy erre a módosított kérdésre igenlő a válasz abban a speciális esetben, amikor m olyan négyzetmentes szám, amelyre teljesül, hogy

$$r \sum_{p \mid m, p \text{ prím}} \frac{1}{p^{1/4}} \leq \frac{1}{\sqrt{10}}.$$

A fejezet során, amikor egyszerre több modulussal is számolunk, a félreértések elkerülése végett $(a)_m$-mel jelöljük az $a \in \mathbb{Z}$ szám modulo m maradékosztályát.

A fejezet eredményei [27]-ben olvashatók.

4.2. Az $a_1 + \cdots + a_n = cd$ egyenlet

Ebben az alfejezetben az $a + b = cd$, és általánosabban az $a_1 + \cdots + a_n = cd$ alakú egyenletek $\mathbb{Z}_m$-beli megoldhatóságát vizsgáljuk. Sárközy a következő tételt bizonyította abban az esetben, amikor a modulus prímszám:

Tétel (Sárközy, [40]). Ha p prímszám, és az

$$\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$$

részhalmazok elemszámainak szorzatára fennáll az

$$|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| > p^3$$

egyenlőtlenség, akkor a (4.1) egyenletnek van olyan megoldása $\mathbb{Z}_p$-ben, amelyre teljesül, hogy

$$a \in \mathcal{A}, b \in \mathcal{B}, c \in \mathcal{C}, d \in \mathcal{D}.$$

Ebben a tételben a p prímszám nem helyettesíthető tetszőleges $m \in \mathbb{N}$ egész számmal. Sőt, a (4.1) egyenletre általában nem teljesül sűrűségi tétel $\mathbb{Z}_m$-ben: megadható olyan $c > 0$ konstans, hogy végtelen sok m esetén létezik olyan $\mathcal{A} \subseteq \mathbb{Z}_m$ halmaz, amelynek legalább cm eleme van, de a (4.1) egyenletnek nincs megoldása $\mathcal{A}$-ban. Tekintsük ugyanis a következő példát:

4.2. Példa. Legyen $4|m$ és álljon $\mathcal{A} \subseteq \mathbb{Z}_m$ a 4-gyel osztva 3 maradékot adó maradékosztályokból:

$$\mathcal{A} = \{3, 7, 11, \ldots, m-1\} \subseteq \mathbb{Z}_m.$$

Az $\mathcal{A}$ halmaz mérete $|\mathcal{A}| = \frac{m}{4}$. Ha $a, b, c, d \in \mathcal{A}$, akkor

$$a + b \equiv 2 \pmod 4,$$

$$cd \equiv 1 \pmod 4,$$

így (4.1) nem oldható meg $\mathcal{A}$-ban.

Azt szeretnénk igazolni, hogy Ramsey-típusú tétel viszont létezik a (4.1) egyenlet esetében. Természetesen tetszőleges színezés esetén triviálisan monokromatikus megoldást kapunk, ha $a = b = c = d$ választás mellett teljesül

$$a + b = 2a = a^2 = cd.$$

Először megmutatjuk, hogy triviális megoldások mindig vannak, és meghatározzuk a számukat. Ehhez az

$$a^2 \equiv 2a \pmod{m}$$

kongruenciát kell megoldanunk. Legyen az m szám kanonikus alakja

$$m = \prod_{i=1}^{r} p_i^{\alpha_i}.$$

A kínai maradéktétel miatt elegendő $\mathbb{Z}_{p_i^{\alpha_i}}$-ben meghatározni a triviális megoldásokat, ugyanis ezek direkt szorzataiból állnak elő a $\mathbb{Z}_m$-beli triviális megoldások. Jelölje az $a^2 \equiv 2a \pmod{p^\alpha}$ kongruencia megoldásainak számát $s(p^\alpha)$. A következő eseteket különböztetjük meg:

- $p > 2$: a $a^2 \equiv 2a \pmod{p^\alpha}$ kongruenciának 2 megoldása van: $a \equiv 0$ és $a \equiv 2$, így $s(p^\alpha) = 2$.
- $p^\alpha = 2$: $a \equiv 0$ az egyetlen megoldás, azaz $s(2) = 1$.
- $p^\alpha = 4$: a 2 megoldás a következő: $a \equiv 0$ és $a \equiv 2$, ezért $s(4) = 2$.
- $p = 2, \alpha \geq 3$: négy megoldás van: $a \equiv 0, 2, 2^{\alpha-1}, 2^{\alpha-1} + 2$, tehát $s(2^\alpha) = 4$.

A kínai maradéktétel szerint az $a+b \equiv cd \pmod{m}$ kongruenciának $\prod_{i=1}^{r} s(p_i^{\alpha_i})$ triviális megoldása van.

A mi célunk természetesen az, hogy megmutassuk, a (4.1) egyenletnek létezik ezektől különböző, nemtriviális megoldása is. A (4.1) egyenletnél általánosabb

$$a_1 + \cdots + a_n = cd \tag{4.3}$$

egyenletről fogjuk igazolni, hogy létezik olyan monokromatikus megoldása, ahol

$$a_1, \ldots, a_n, c, d \in \mathbb{Z}_m$$

páronként különbözők. Ezeket a megoldásokat, ahol $a_1, \ldots, a_n, c, d \in \mathbb{Z}_m$ páronként különbözők, primitív megoldásoknak fogjuk nevezni.

A bizonyítás Rado tételének előző fejezetben ismertetett alakjának felhasználásán alapul ([34]). A bizonyítás során használni fogjuk a következő észrevételt:

4.3. Lemma. *Legyen $T \in \mathbb{N}$ és $N = T^T$. Ha $m > N$, akkor az m számnak van T-nél nagyobb prímhatvány osztója.*

Bizonyítás. Tegyük fel, hogy az m számnak nincsen T-nél nagyobb prímhatvány osztója. Ekkor m minden prímosztója legfeljebb T, ezért m legfeljebb T darab prímhatvány szorzata. Mivel ezek a prímhatványok nem nagyobbak, mint T, ezért $m \leq T^T$, ami igazolja az állításunkat. □

4.4. Tétel. *Tetszőleges $n, r \in \mathbb{N}$ esetén létezik olyan $N = N(n, r)$, hogy minden $N < m \in \mathbb{N}$ egész szám, és $\mathbb{Z}_m$ minden r-színezése esetén van primitív monokromatikus megoldása a (4.3) egyenletnek $\mathbb{Z}_m$-ben.*

Bizonyítás. Tekintsük $\mathbb{Z}_m$ egy tetszőleges r-színezését, és először tegyük fel, hogy $n \geq 2$. Legyen $C > r^4(n+2)^4$ egy konstans, melyet később fogunk meghatározni. A 4.3. Lemmát $T = C^3$ választással alkalmazva azt kapjuk, hogy ha $m > N = T^T$, akkor m-nek van T-nél nagyobb prímhatvány osztója.

Megmutatjuk, hogy $N = T^T$ kielégíti a tétel feltételeit. Két esetet különböztetünk meg aszerint, hogy az m szám 4.3. Lemma által garantált prímhatvány osztója prímszám-e vagy sem.

Először tegyük fel, hogy

$$p > r^4(n+2)^4$$

az m szám egy olyan prímosztója, melyre $p^2 \nmid m$. Ekkor p és m/p relatív prímek, hiszen $p \nmid m/p$. Definiáljuk az $(x_i)_m$ modulo m maradékosztályt $1 \leq i \leq p$ esetén a következő kongruenciákkal:

$$x_i \equiv i \pmod{p},$$

$$x_i \equiv 0 \pmod{m/p}.$$

Definiáljuk $\mathbb{Z}_p$ egy r-színezését $\mathbb{Z}_m$ megadott r-színezése alapján a következő módon: ha $1 \leq i \leq p$, legyen $(i)_p \in \mathbb{Z}_p$ színe az $(x_i)_m$ maradékosztály színe. Mivel $\mathbb{Z}_p$-t r színnel színeztük, ezért ki tudunk választani legalább $\frac{p}{r}$ egyforma színű elemet. Jelölje ennek a legalább $\frac{p}{r}$ egyforma színű elemnek a halmazát $\mathcal{S}$. Osszuk fel az $\mathcal{S} \subseteq \mathbb{Z}_p$ halmazt $n+2$ páronként diszjunkt halmazra úgy, hogy ezek közül semelyik kettőnek az elemszáma ne térjen el 1-nél többel. Legyenek ezek a halmazok:

$$\mathcal{S}_1, \ldots, \mathcal{S}_{n+2} \subseteq \mathcal{S}.$$

Mivel
$$p \geq r^4(n+2)^4 \geq 2r(n+2),$$
ezért mindegyik $\mathcal{S}_i$ halmaz méretére igaz, hogy
$$|\mathcal{S}_i| \geq \left\lfloor \frac{p}{r(n+2)} \right\rfloor \geq \frac{p}{2r(n+2)}.$$
Definiáljuk az $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ halmazokat a következő módon:
$$\mathcal{A} = \mathcal{S}_1,$$
$$\mathcal{B} = \mathcal{S}_2 + \cdots + \mathcal{S}_n = \{s_2 + \cdots + s_n \mid s_2 \in \mathcal{S}_2, \ldots, s_n \in \mathcal{S}_n\},$$
$$\mathcal{C} = \mathcal{S}_{n+1},$$
$$\mathcal{D} = \mathcal{S}_{n+2}.$$
Mivel $p > r^4(n+2)^4$, ezért
$$|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| \geq \left(\frac{p}{r(n+2)}\right)^4 > p^3,$$
így Sárközy tétele alkalmazható, tehát léteznek olyan
$$a \in \mathcal{A}, b \in \mathcal{B}, c \in \mathcal{C}, d \in \mathcal{D}$$
számok, melyekre $a + b = cd$ teljesül $\mathbb{Z}_p$-ben. Mivel $b \in \mathcal{B}$, ezért $b = a_2 + \cdots + a_n$ teljesül alkalmas $a_i \in \mathcal{S}_i$ $(2 \leq i \leq n)$ elemekkel. Legyen $a_1 = a$. Azt kaptuk tehát, hogy léteznek
$$a_1, \ldots, a_n, c, d \in \{1, 2, \ldots, p\}$$
egész számok úgy, hogy az általuk reprezentált modulo p maradékosztályok színe egyforma, továbbá teljesül a következő kongruencia:
$$a_1 + \cdots + a_n \equiv cd \pmod{p}.$$
Az
$$(x_{a_1})_m, \ldots, (x_{a_n})_m, (x_c)_m, (x_d)_m \in \mathbb{Z}_m$$
modulo m maradékosztályok színe megegyezik az
$$(a_1)_p, \ldots, (a_n)_p, (c)_p, (d)_p \in \mathbb{Z}_p$$

modulo p maradékosztályok színével $\mathbb{Z}_p$ színezésének definíciója miatt. Ugyanezért ezek a modulo m maradékosztályok páronként különbözők, hiszen

$$(a_1)_p, \dots, (a_n)_p, (c)_p, (d)_p \in \mathbb{Z}_p$$

is páronként különbözők. Végül, az $(x_{a_1})_m, \dots, (x_{a_n})_m, (x_c)_m, (x_d)_m$ maradékosztályok kielégítik a (4.3) egyenletet, hiszen:

- Mivel minden i-re $x_i \equiv 0 \pmod{m/p}$, ezért

$$(x_{a_1})_{m/p} \dots (x_{a_n})_{m/p} \equiv (x_c)_{m/p}(x_d)_{m/p} \pmod{m/p}.$$

- Mivel minden i-re $x_i \equiv i \pmod{p}$, és

$$a_1 \dots a_n \equiv cd \pmod{p},$$

ezért

$$(x_{a_1})_p \dots (x_{a_n})_p \equiv (x_c)_p(x_d)_p \pmod{p}.$$

Tehát az

$$(x_{a_1})_m, \dots, (x_{a_n})_m, (x_c)_m, (x_d)_m \in \mathbb{Z}_m$$

maradékosztályok (4.3) egy primitív monokromatikus megoldását alkotják.

Most rátérünk arra az esetre, amikor az m szám egy prímhatvány (de nem prím) osztójára $p^t \geq C^3$ teljesül. Azaz $p^t | m$, ahol $t \geq 2$, és feltehető, hogy t a legnagyobb olyan egész szám, amelyre $p^t | m$. Legyen $t_0 = \lfloor t/2 \rfloor$. Mivel $t_0 \geq t/3$, ezért $p^{t_0} \geq C$. Be fogjuk látni, hogy az

$$a_1 + \dots + a_n \equiv cd \pmod{m}$$

egyenletnek van primitív monokromatikus megoldása már az

$$\left(y \cdot \frac{m}{p^{t_0}} + n \right)_m$$

alakú maradékosztályok körében is. Vegyük észre, hogy az

$$\left(\alpha_1 \cdot \frac{m}{p^{t_0}} + n \right)_m + \dots + \left(\alpha_n \cdot \frac{m}{p^{t_0}} + n \right)_m \equiv$$
$$\equiv \left(\gamma \cdot \frac{m}{p^{t_0}} + n \right)_m \left(\delta \cdot \frac{m}{p^{t_0}} + n \right)_m \pmod{m}$$

kongruencia ekvivalens az

$$\alpha_1 + \cdots + \alpha_n \equiv n\gamma + n\delta \pmod{p^{t_0}}$$

kongruenciával. Következő lépésként definiáljuk $\mathbb{N}$ egy r-színezését $\mathbb{Z}_m$ megadott r-színezéséből kiindulva. Legyen az $y \in \mathbb{N}$ szám színe az $\left(y \cdot \frac{m}{p^{t_0}} + n\right)_m \in \mathbb{Z}_m$ maradékosztály színe. Tekintsük a következő egész számokat:

$$\alpha_i = (1-n) + 2(i-1) \ (i = 1, \ldots, n \text{ esetén}), \gamma = n, \delta = -n.$$

Könnyen ellenőrizhetjük, hogy az $\alpha_1, \ldots, \alpha_n, \gamma, \delta$ egész számok páronként különbözők, és kielégítik az

$$\alpha_1 + \cdots + \alpha_n - n\gamma - n\delta = 0 \tag{4.4}$$

egyenletet. Tehát a (4.4) egyenletnek van páronként különböző számokból álló megoldása $\mathbb{Z}$-ben. Ezen kívül az $\alpha_1, \ldots, \alpha_n, \gamma$ változók együtthatóira $1 + \cdots + 1 - n = 0$ is teljesül, vagyis a (4.4) egyenlet kielégíti Rado tételének feltételeit, ezért ha K értékét elegendően nagynak választjuk, mondjuk $K \geq K_0$, akkor (4.4)-nek az $\{1, 2, \ldots, K\}$ halmaz tetszőleges r-színezése esetén van primitív monokromatikus megoldása $\{1, 2, \ldots, K\}$-ban. Válasszuk meg C értékét N definíciójában úgy, hogy $C \geq K_0$ teljesüljön. Rado tétele szerint léteznek olyan

$$\alpha_1, \ldots, \alpha_n, \gamma, \delta \in \{1, 2, \ldots, C\}$$

páronként különböző egész számok, melyek egyforma színűek, és kielégítik az

$$\alpha_1 + \cdots + \alpha_n - n\gamma - n\delta = 0$$

egyenletet. Ez azt jelenti, hogy az

$$a_i = \left(\alpha_i \cdot \frac{m}{p^{t_0}} + n\right)_m, c = \left(\gamma \cdot \frac{m}{p^{t_0}} + n\right)_m, d = \left(\delta \cdot \frac{m}{p^{t_0}} + n\right)_m$$

maradékosztályok a (4.3) egyenlet egy primitív monokromatikus megoldását alkotják, ugyanis:

- Mivel az
$$\alpha_1, \ldots, \alpha_n, \gamma, \delta \in \{1, 2, \ldots, C\}$$
számok különbözők és $p^{t_0} \geq C$, ezért $a_1, \ldots, a_n, c, d \in \mathbb{Z}_m$ is különbözők.

- Az $a_1, \dots, a_n, c, d$ maradékosztályok színe megegyezik az α_1, ..., α_n, γ, δ egész számok színével $\mathbb{N}$ színezésének definíciója következtében.

Ezzel megmutattuk, hogy ha $m > N = T^T$, akkor (4.3)-nak van primitív monokromatikus megoldása $\mathbb{Z}_m$-ben.

Végül, vizsgáljuk meg az $n = 1$ esetet. Schur tétele szerint minden $r \in \mathbb{N}$ számhoz létezik olyan $M = M(r)$, hogy $\mathbb{N}$ minden r-színezése esetén van páronként különböző számokból álló monokromatikus megoldása az $\alpha = \gamma + \delta$ egyenletnek $\{1, 2, \dots, M\}$-ben. Tegyük fel, hogy $2^M < m$, és tekintsük $\mathbb{Z}_m$ egy tetszőleges r-színezését. Definiáljuk $\mathbb{N}$ egy r-színezését a következő módon: legyen $a \in \mathbb{N}$ színe $(2^a)_m \in \mathbb{Z}_m$ maradékosztály színe. Rado tétele szerint léteznek olyan páronként különböző $\alpha, \gamma, \delta \in \{1, 2, \dots, M\}$ számok, amelyek egyforma színűek, és teljesül, hogy $\alpha = \gamma + \delta$. Ekkor

$$a_1 = (2^\alpha)_m, c = (2^\gamma)_m, d = (2^\delta)_m$$

számok az $a_1 = cd$ egyenlet egy primitív monokromatikus megoldását alkotják $\mathbb{Z}_m$-ben.

□

4.3. Az $ab + 1 = cd$ egyenlet

Ebben az alfejezetben az $ab+1 = cd$ egyenlet $\mathbb{Z}_m$-beli megoldhatóságát vizsgáljuk. Először megmutatjuk, hogy ha az m számnak van „kicsi" prímosztója, akkor nem igaz Ramsey-típusú tétel a klasszikus értelemben: ha a színek r számát rögzítjük, akkor is végtelen sok olyan m létezik, melyre megadható $\mathbb{Z}_m$-nek olyan r-színezése, hogy (4.2)-nek nincs monokromatikus megoldása.

4.5. Példa. Legyen $p|m$ és legyen $(x)_m \in \mathbb{Z}_m$ színe az x szám modulo p maradékosztálya. Ha

$$(a)_m, (b)_m, (c)_m, (d)_m \in \mathbb{Z}_m$$

egyforma színűek, akkor

$$ab \equiv cd \pmod{p},$$

és így $ab + 1 \neq cd$ ($\mathbb{Z}_m$-ben).

Ebben a példában $\mathbb{Z}_m$-et p színnel színeztük, ahol p az m szám egy tetszőleges prímosztója volt, és azt kaptuk, hogy az $ab+1 = cd$ egyenletnek nincsen monokromatikus megoldása. Ez azt jelenti, hogy Ramsey-típusú tétel csak akkor teljesülhet, ha az m szám legkisebb prímosztója, amit $p(m)$-mel fogunk jelölni, nagyobb, mint a színek száma. Az előzőhöz hasonló ellenpéldákat kizárhatjuk, ha a problémát újrafogalmazzuk a következő módon:

4.6. Probléma. Igaz-e Ramsey-típusú eredmény az $ab + 1 = cd$ egyenlet $\mathbb{Z}_m$-beli megoldhatóságára, ha a színek r száma rögzített, és $p(m)$ elegendően nagy: $p(m) > N(r)$?

Megmutatjuk, hogy a válasz igen, ha m négyzetmentes, és teljesül a következő egyenlőtlenség:

$$r \sum_{p|m} \frac{1}{p^{1/4}} \leq \frac{1}{\sqrt{10}}.$$

Ez az új feltétel természetesen adódik Sárközy alábbi tételéből:

Tétel (Sárközy, [39]). Ha p prím, és az $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ halmazokra teljesül az

$$|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| > 100p^3$$

egyenlőtlenség, akkor a (4.2) egyenletnek van olyan megoldása $\mathbb{Z}_p$-ben, amelyre $a \in \mathcal{A}, b \in \mathcal{B}, c \in \mathcal{C}, d \in \mathcal{D}$.

Most már készen állunk arra, hogy megoldjuk a 4.6. Problémát a következő, erősebb feltételek mellett:

4.7. Tétel. *Legyen az $m = p_1 \dots p_s$ szám s különböző prímszám szorzata. Legyen $\mathcal{A} \subseteq \mathbb{Z}_m$, és legyen $\alpha = \frac{|\mathcal{A}|}{m}$. Ha*

$$\sum_{j=1}^{s} \frac{1}{p_j^{1/4}} \leq \frac{\alpha}{\sqrt{10}},$$

akkor léteznek olyan $a, b, c, d \in \mathcal{A}$ számok, amelyekre teljesül az $ab + 1 = cd$ egyenlet.

Bizonyítás. A bizonyítás alapötlete az, hogy az $ab+1 = cd$ egyenlet $\mathbb{Z}_m$-beli megoldásához úgy jutunk el, hogy lépésről lépésre megoldjuk az

$$ab + 1 \equiv cd \pmod{p_i} \; (1 \leq i \leq s)$$

kongruenciarendszert. Célunk az, hogy végül olyan megoldást kapjunk, melyre $(a)_m, (b)_m, (c)_m, (d)_m$ az $\mathcal{A}$ halmazba esnek. Először igazoljuk a következő

segédállítást:
Legyen $m = m_1 m_2 \dots m_s$, ahol $m_1, m_2, \dots, m_s$ páronként relatív prímek. Legyen
$$\mathcal{A} \subseteq \mathbb{Z}_m = \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_s},$$
vezessük be az $\alpha = \frac{|\mathcal{A}|}{m}$ jelölést, és tegyük fel, hogy az $\alpha_1, \dots, \alpha_s \geq 0$ számokra teljesül, hogy
$$\alpha_1 + \dots + \alpha_s \leq \alpha.$$
Ekkor léteznek olyan $\mathcal{A}_1 \subseteq \mathbb{Z}_{m_1}$, $\mathcal{A}_j(a_1, \dots, a_{j-1}) \subseteq \mathbb{Z}_{m_j}$ halmazok (tetszőleges $a_1 \in \mathcal{A}_1$, $a_2 \in \mathcal{A}_2(a_1)$, és így tovább, $a_{j-1} \in \mathcal{A}_{j-1}(a_1, \dots, a_{j-2})$ esetén), melyekre teljesülnek a következő feltételek:

- $|\mathcal{A}_1| \geq \alpha_1 m_1$
- Minden $2 \leq j \leq r$, minden $a_1 \in \mathcal{A}_1$, minden $a_2 \in \mathcal{A}_2(a_1)$, minden $a_3 \in \mathcal{A}_3(a_1, a_2)$, és így tovább, minden $a_{j-1} \in \mathcal{A}_{j-1}(a_1, \dots, a_{j-2})$ esetén az $\mathcal{A}_j(a_1, \dots, a_{j-1})$ halmaz mérete legalább $\alpha_j m_j$.
- Ha $a_1 \in \mathcal{A}_1, a_2 \in \mathcal{A}_2(a_1), \dots, a_s \in \mathcal{A}_s(a_1, \dots, a_{s-1})$, akkor
$$(a_1, \dots, a_s) \in \mathcal{A}.$$

Tehát az
$$\mathcal{A}_j(a_1, \dots, a_{j-1}) \subseteq \mathbb{Z}_{m_j}$$
halmaz az
$$(a_1, \dots, a_{j-1}) \in \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_{j-1}}$$
elem legalább $\alpha_j m_j$ féle j-edik koordinátával való lehetséges folytatását tartalmazza. Pontosabban, legalább $\alpha_j m_j$ féle $a_j \in \mathbb{Z}_{m_j}$ elemet írhatunk j-edik koordinátaként az $(a_1, \dots, a_{j-1})$ vektor után úgy, hogy az s-edik lépés után csak az
$$\mathcal{A} \subseteq \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_s}$$
halmazba eső vektorokat kapjunk.

Ezt az állítást s-re vonatkozó teljes indukcióval bizonyítjuk. Ha $s = 1$, akkor az állítás triviálisan teljesül. Legyen $s = 2$. Minden $a_1 \in \mathbb{Z}_{m_1}$ esetén legyen
$$\mathcal{A}_2(a_1) = \{a_2 : (a_1, a_2) \in \mathcal{A}\}.$$

Tekintsük a következő halmazt:

$$\mathcal{A}_1 = \{a_1 \in \mathbb{Z}_{m_1} : |\mathcal{A}_2(a_1)| \geq \alpha_2 m_2\}.$$

Mivel

$$\mathcal{A} = \bigcup_{a_1 \in \mathcal{A}_1} \{a_1\} \times \mathcal{A}(a_1) \cup \bigcup_{a_1 \in \mathbb{Z}_{m_1} \setminus \mathcal{A}_1} \{a_1\} \times \mathcal{A}(a_1),$$

ezért

$$\alpha m_1 m_2 = |\mathcal{A}| \leq |\mathcal{A}_1| m_2 + (m_1 - |\mathcal{A}_1|)\alpha_2 m_2 \leq |\mathcal{A}_1| m_2 + \alpha_2 m_1 m_2.$$

Tehát az $\mathcal{A}_1$ halmaz mérete legalább $\alpha_1 m_1$, és $\mathcal{A}_1$ definíciójából triviálisan következik, hogy minden $a_1 \in \mathcal{A}_1$ esetén $\mathcal{A}_2(a_1)$ elemszáma legalább $\alpha_2 m_2$, valamint tetszőleges $a_1 \in \mathcal{A}_1, a_2 \in \mathcal{A}_2(a_1)$ esetén $(a_1, a_2) \in \mathcal{A}$. Ezzel $s = 2$-re is igazoltuk az állítást. Ezt a lépést ismételten alkalmazva kapjuk, hogy az állítás tetszőleges $s > 2$ esetén is igaz.

Ez azt jelenti, hogy $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_s}$-ben legalább $\alpha_1 m_1$ féle első koordinátát választhatunk, ezeket az $\mathcal{A}_1$ halmaz tartalmazza. Minden $a_1 \in \mathcal{A}_1$ esetén legalább $\alpha_2 m_2$ féle második koordinátát választhatunk, ezeket az $\mathcal{A}_2(a_1)$ halmaz tartalmazza. És így tovább, végül $\alpha_s m_s$ féle s-edik koordinátát választhatunk úgy, hogy az összes $(a_1, \ldots, a_s)$ alakú vektor, amit kaptunk $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_s}$-ben az $\mathcal{A}$ halmazba essen.

Legyen $m = p_1 \ldots p_s$. Mivel a kínai maradéktétel szerint

$$\mathbb{Z}_m = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s},$$

ezért egy tetszőleges a szám modulo m maradékosztálya egyértelműen megfeleltethető egy rendezett s-esnek, ahol a j-edik koordináta az a szám modulo p_j maradékosztálya:

$$a \leftrightarrow (a_1, \ldots, a_s),$$

ahol $(a)_{p_j} = (a_j)_{p_j}$ minden $1 \leq j \leq s$ esetén. Az $ab + 1 = cd$ egyenlet megoldása $\mathcal{A} \subseteq \mathbb{Z}_m$-ben ekvivalens probléma az

$$a_i b_i + 1 = c_i d_i \ (\mathbb{Z}_{p_i} - \text{ben})(1 \leq i \leq s)$$

kongruenciarendszer olyan megoldásával, amelyre

$$(a_1, \ldots, a_s), (b_1, \ldots, b_s), (c_1, \ldots, c_s), (d_1, \ldots, d_s) \in \mathcal{A}.$$

Az előbb igazolt állítást $m_i = p_i$ választással alkalmazva azt kapjuk, hogy ha az

$$\alpha_1, \dots, \alpha_s \geq 0$$

számok kielégítik az

$$\alpha_1 + \cdots + \alpha_s \leq \alpha$$

egyenlőtlenséget, akkor választhatók olyan

$$\mathcal{A}_j(a_1, \dots, a_{j-1}) \subseteq \mathbb{Z}_{p_j}$$

halmazok, melyekre a következő feltételek teljesülnek:

- $|\mathcal{A}_1| \geq \alpha_1 p_1$.
- Minden $2 \leq j \leq s$, minden $a_1 \in \mathcal{A}_1$, minden $a_2 \in \mathcal{A}_2(a_1)$, minden $a_3 \in \mathcal{A}_3(a_1, a_2)$, és így tovább, minden $a_{j-1} \in \mathcal{A}_{j-1}(a_1, \dots, a_{j-2})$ esetén az $\mathcal{A}_j(a_1, \dots, a_{j-1})$ halmaz mérete legalább $\alpha_j p_j$.
- Ha $a_1 \in \mathcal{A}_1, a_2 \in \mathcal{A}_2(a_1), \dots, a_s \in \mathcal{A}_s(a_1, \dots, a_{s-1})$, akkor

  $$(a_1, \dots, a_s) \in \mathcal{A}.$$

A következő lépés Sárközy tételének ismételt alkalmazása lesz. Ahhoz, hogy alkalmazhassuk, az

$$(\alpha_j p_j)^4 \geq 100 p_j^3 \ (1 \leq j \leq s) \tag{4.5}$$

egyenlőtlenségeknek teljesülnie kell majd. Legyen tehát minden $1 \leq j \leq s$ esetén

$$\alpha_j = \frac{\sqrt{10}}{p_j^{1/4}}.$$

Mivel

$$\sum_{j=1}^{s} \alpha_j = \sqrt{10} \sum_{j=1}^{s} \frac{1}{p_j^{1/4}} \leq \alpha,$$

ezért az előző segédállítás alkalmazható, és választhatók a feltételeknek megfelelő $\mathcal{A}_j(a_1, \dots, a_{j-1})$ halmazok. Mivel $|\mathcal{A}_1| \geq \alpha_1 p_1$ és (4.5) is teljesül, ezért Sárközy tétele szerint az

$$a_1 b_1 + 1 = c_1 d_1 \ (\mathbb{Z}_{p_1}\text{-ben})$$

egyenlet megoldható $\mathcal{A}_1$-ben. Rögzítsünk egy megoldást: a_1, b_1, c_1, d_1. Mivel az

$$\mathcal{A}_2(a_1), \mathcal{A}_2(b_1), \mathcal{A}_2(c_1), \mathcal{A}_2(d_1)$$

halmazok mindegyikének mérete legalább $\alpha_2 p_2$, és (4.5) teljesül, így

$$a_2 b_2 + 1 = c_2 d_2 \ (\mathbb{Z}_{p_2}\text{-ben})$$

egyenletnek van olyan megoldása, amelyre teljesül, hogy

$$a_2 \in \mathcal{A}_2(a_1), b_2 \in \mathcal{A}_2(b_1), c_2 \in \mathcal{A}_2(c_1), d_2 \in \mathcal{A}_2(d_1).$$

Rögzítsünk egy megoldást: a_2, b_2, c_2, d_2. Az általános lépésben

$$a_1, \ldots, a_j, b_1, \ldots, b_j, c_1, \ldots, c_j, d_1, \ldots, d_j$$

számokat már rögzítettük. Mivel az

$$\mathcal{A}_{j+1}(a_1, \ldots, a_j), \mathcal{A}_{j+1}(b_1, \ldots, b_j), \mathcal{A}_{j+1}(c_1, \ldots, c_j), \mathcal{A}_{j+1}(d_1, \ldots, d_j)$$

halmazok mérete legalább $\alpha_{j+1} p_{j+1}$, és (4.5) teljesül, ezért az

$$a_{j+1} b_{j+1} + 1 = c_{j+1} d_{j+1} \ (\mathbb{Z}_{p_{j+1}}\text{-ben})$$

egyenletnek van olyan megoldása, amelyre teljesül, hogy

$$a_{j+1} \in \mathcal{A}_{j+1}(a_1, \ldots, a_j), b_{j+1} \in \mathcal{A}_{j+1}(b_1, \ldots, b_j),$$
$$c_{j+1} \in \mathcal{A}_{j+1}(c_1, \ldots, c_j), d_{j+1} \in \mathcal{A}_{j+1}(d_1, \ldots, d_j).$$

Végül, mivel az

$$\mathcal{A}_s(a_1, \ldots, a_{s-1}), \mathcal{A}_s(b_1, \ldots, b_{s-1}), \mathcal{A}_s(c_1, \ldots, c_{s-1}), \mathcal{A}_s(d_1, \ldots, d_{s-1})$$

halmazok mérete legalább $\alpha_s p_s$, ezért az

$$a_s b_s + 1 = c_s d_s \ (\mathbb{Z}_{p_s}\text{-ben})$$

egyenletnek van olyan megoldása, melyre

$$a_s \in \mathcal{A}_s(a_1, \ldots, a_{s-1}), b_s \in \mathcal{A}_s(b_1, \ldots, b_{s-1}),$$
$$c_s \in \mathcal{A}_s(c_1, \ldots, c_{s-1}), d_s \in \mathcal{A}_s(d_1, \ldots, d_{s-1}).$$

Tehát az

$$a = (a_1, \ldots, a_s), b = (b_1, \ldots, b_s), c = (c_1, \ldots, c_s), d = (d_1, \ldots, d_s) \in \mathcal{A}$$

számokra fennáll az

$$ab + 1 = cd \text{ } (\mathbb{Z}_m\text{-ben})$$

egyenlőség. Ezzel a tétel állítását igazoltuk.

□

4.8. Következmény. *Legyen az $m = p_1 \ldots p_s$ szám s különböző prímszám szorzata. Ha*

$$r \sum_{j=1}^{s} \frac{1}{p_j^{1/4}} \leq \frac{1}{\sqrt{10}},$$

akkor $\mathbb{Z}_m$ minden r-színezése esetén van monokromatikus megoldása az $ab + 1 = cd$ egyenletnek.

Bizonyítás. A 4.7. Tételt alkalmazzuk a legnagyobb színosztályra. □

5. fejezet

Multiplikatív Sidon-típusú sorozatok

Ebben a fejezetben azt vizsgáljuk, hogy az $\{1, 2, \ldots, n\}$ halmaznak legfeljebb mekkora részhalmazát lehet úgy kiválasztani, hogy minden szám legfeljebb egyféleképpen álljon elő a halmaz k elemének szorzataként. Erdős a $k = 2$ esetet vizsgálta, ezeket a halmazokat multiplikatív Sidon-sorozatoknak nevezzük: [9]-ben $\pi(n) + c_1 n^{3/4}/(\log n)^{3/2}$ méretű konstrukciót adott, és igazolta, hogy egy ilyen tulajdonságú halmaz elemszáma legfeljebb $\pi(n) + c_2 n^{3/4}$ lehet. 31 évvel később [11]-ben a felső becslést $\pi(n) + c_2 n^{3/4}/(\log n)^{3/2}$-re javította, így az alsó és felső becslésben már nem csak a fő tag egyezik, hanem a hibatagok is csak konstans szorzóban térnek el. Mi ennek a problémának az általánosításaként azt a kérdést vizsgáljuk, hogy legfeljebb hány eleme lehet az $\{1, 2, \ldots, n\}$ halmaz egy olyan részhalmazának, melynek nem választható ki $2k$ különböző eleme úgy, hogy rájuk $a_1 \ldots a_k = b_1 \ldots b_k$ teljesüljön. Ezt a maximális elemszámot $G_k(n)$-nel jelöljük. Az 5.11. Tételben megmutatjuk, hogy $k = 3$ esetén

$$\pi(n) + \pi(n/2) + cn^{2/3}/(\log n)^{4/3} \leq G_3(n) \leq$$
$$\leq \pi(n) + \pi(n/2) + \left(\frac{2e}{3} + \varepsilon\right) \cdot n^{2/3} \cdot \frac{\log n}{\log\log n}.$$

A $k = 4$ esetben pedig a következő becsléseket bizonyítjuk az 5.12. és 5.13. Tételekben:

$$\pi(n) + n^{3/5}/(\log n)^{6/5} \leq G_4(n) \leq \pi(n) + (10 + \varepsilon)n^{2/3}.$$

A $k=3$-ra és 4-re kapott eredményekből tetszőleges k-ra vonatkozó felső becsléseket vezetünk le az 5.15. Következményben.

Amennyiben csak annyit követelnénk meg, hogy az egyenlet két oldalán szereplő tényezők $\{a_1,\ldots,a_k\}$, illetve $\{b_1,\ldots,b_k\}$ halmaza különböző legyen, az additív Sidon-sorozatok általánosításaként kapott $B_g[1]$-sorozatok multiplikatív megfelelőjét kapnánk. A $G_k(n)$-ről szóló tételek következményeként ezek maximális elemszámára is becsléseket adunk az 5.19. Következményben.

Erdős szintén vizsgálta a következő, rokon problémát: az $\{1,2,\ldots,n\}$ halmaznak legfeljebb mekkora részhalmaza választható ki úgy, hogy semelyik kiválasztott elem ne ossza k másik szorzatát. Ha az $a_1\ldots a_k=b_1\ldots b_k$ egyenletnek van páronként különböző számokból álló megoldása, akkor van olyan szám, amely osztója k másik szorzatának, így $G_k(n)$ felső becslést ad ennél a problémánál. Erdős $k=2$ esetén először a $\pi(n)+2n^{2/3}$ felső becslést igazolta. Majd [9]-ben ezt $\pi(n)+cn^{2/3}/(\log n)^2$-re javította, és ugyanilyen alakú alsó becslést is bizonyított egy másik pozitív c konstanssal. Chan, Győri, Sárközy [5]-ben $2\le k\le\frac{\log n}{6\log\log n}$ esetén $\pi(n)+\frac{n^{2/(k+1)}}{8k^2(\log n)^2}$ elemszámú a feltételt kielégítő halmazt konstruáltak, valamint $k=3$ esetén a $\pi(n)+cn^{1/2}/(\log n)^2$ felső becslést adták. Chan [4] a $2\le k\le\frac{1}{6}\sqrt{\frac{\log n}{\log\log n}}$ feltétel mellett $\pi(n)+c\frac{n^{\frac{2}{k+1}}}{(k+1)^2(\log n)^2}$ alakban felírható alsó és felső becslést adott.

Erdős, Sárközy és T. Sós [12] azt vizsgálták, hogy az $\{1,2,\ldots,n\}$ halmaznak legfeljebb hány eleme választható ki úgy, hogy közülük semelyik k darab különbözőnek a szorzata ne legyen négyzetszám. Ezt a maximális elemszámot $F_k(n)$-nel jelölték. Az F és G függvényekre tetszőleges k,n mellett fennáll az $F_{2k}(n)\le G_k(n)$ egyenlőtlenség, ugyanis ha az $a_1\ldots a_k=b_1\ldots b_k$ egyenletnek van páronként különböző számokból álló megoldása, akkor ennek a $2k$ számnak a szorzata négyzetszám. Erdős, Sárközy és T. Sós megmutatták, hogy $k=6$ esetén

$$\pi(n)+\pi(n/2)+c_1n^{2/3}/(\log n)^{4/3}\le F_6(n)\le\pi(n)+\pi(n/2)+c_2n^{7/9}\log n.$$

Továbbá megjegyezték, hogy a bizonyításukban használt gráfelméleti lemmájuk megjavításával a $\pi(n)+\pi(n/2)+c_2n^{2/3}\log n$ felső becslés is igazolható lenne, így az alsó és a felső becslésben az egyforma fő tag mellett már a hibatagok is csak log-hatvány szorzóban térnének el. Győri [18] megjavította ezt a gráfelméleti lemmát, és ezzel bebizonyította a kívánt becslést. Erdős, Sárközy és T. Sós $k=8$ esetén a

$$\pi(n)+c_1n^{4/7}/(\log n)^{8/7}\le F_8(n)\le\pi(n)+c_2n^{3/4}/(\log n)^{-3/2}$$

becsléseket igazolták. Mi $F_{2k}(n)$-re felső becslést adunk a $G_k(n)$ függvényre vonatkozó becslésünk következményeként, valamint alsó becslést adunk $F_8(n)$-re. A $k = 3$ esetben Győri felső becslésén egy $\log\log n$-es faktort javítunk, és belátjuk az 5.16. Következményben, hogy:

$$F_6(n) \le \pi(n) + \pi(n/2) + \left(\frac{2e}{3} + \varepsilon\right) \cdot n^{2/3} \cdot \frac{\log n}{\log\log n}$$

is teljesül. A $k = 4$ esetben az alsó és felső becslés hibatagját is lényegesen megjavítjuk az 5.16. és az 5.17. Következményekben. Megmutatjuk, hogy

$$\pi(n) + c_2 n^{3/5}/(\log n)^{7/10} \le F_8(n) \le \pi(n) + (10 + \varepsilon)n^{2/3}.$$

Azaz ebben a fejezetben nevezetes multiplikatív Sidon-sorozatokkal kapcsolatos problémákat vizsgálunk megjavítva Erdős, Sárközy, T. Sós és Győri becsléseit. A fejezet eredményei [28]-ban olvashatók.

5.1. Felhasznált lemmák

A bizonyítás során szükségünk a következő lemmákra.
Jelölje $ex(n, C_k)$ a k hosszú kört nem tartalmazó n csúcsú gráfok maximális élszámát, valamint jelölje $ex(u, v, C_{2k})$ az olyan páros gráfok maximális élszámát, amelyek nem tartalmaznak $2k$ hosszú kört, és a két független csúcsosztály elemszáma u, illetve v.

5.1. Lemma. *Legyen n pozitív egész szám. Ekkor*

$$\frac{1}{3}n^{3/2} < ex(n, C_4) < \frac{n}{4}(1 + \sqrt{4n - 3}),$$

ha n elegendően nagy.

Bizonyítás. Reiman [35]-ben igazolja a felső becslést, valamint tetszőleges p prímszám esetén konstruál $n = p^2 + p + 1$ pontú C_4-mentes gráfot, melynek $\frac{1}{2}p(p + 1)^2 \sim \frac{1}{2}n^{3/2}$ éle van. Ebből az alsó becslés is könnyen következik, hiszen ha a legnagyobb olyan p prímszámot vesszük, melyre $p^2 + p + 1 \le n$, akkor a $p^2 + p + 1$-hez tartozó gráfot $n - p^2 - p - 1$ izolált ponttal kiegészítve megfelelő gráfot kapunk. □

5.2. Lemma. *Legyen n pozitív egész szám. Ekkor*

$$ex(n, C_6) < 0,6272n^{\frac{4}{3}},$$

ha n elegendően nagy.

Bizonyítás. A lemma bizonyítása megtalálható Füredi, Naor és Verstraëte [13] cikkében. □

5.3. Lemma. *Legyen n pozitív egész szám. Ekkor*

$$ex(n, C_{2k}) < 100kn^{\frac{k+1}{k}}.$$

Bizonyítás. Bizonyítása megtalálható Bondy és Simonovits [2] cikkében. □

5.4. Lemma. *Legyenek u és v pozitív egész számok. Ekkor*

$$ex(u, v, C_6) \leq (uv)^{2/3} + 16(u + v).$$

Bizonyítás. A lemma bizonyítása megtalálható Füredi, Naor és Verstraëte [13] cikkében. □

5.5. Lemma. *Legyenek u és v pozitív egész számok, amelyekre $v \leq u$ teljesül. Ekkor*

$$ex(u, v, C_6) < 2u + v^2/2.$$

Bizonyítás. Bizonyítása megtalálható Győri [18] cikkében. □

5.6. Lemma. *Legyenek u és v pozitív egész számok. Ekkor tetszőleges $k \geq 2$ esetén*

$$ex(u, v, C_{2k}) \leq (2k-3)[(uv)^{\frac{k+1}{k}} + u + v], \text{ ha } k \text{ páratlan},$$

$$ex(u, v, C_{2k}) \leq (2k-3)[u^{\frac{k+2}{2k}} v^{\frac{1}{2}} + u + v], \text{ ha } k \text{ páros}.$$

Bizonyítás. Bizonyítása megtalálható Naor és Verstraëte [25] cikkében. □

5.7. Lemma. *Létezik olyan $c > 0$ konstans, hogy ha n elég nagy, akkor megadható olyan 8 bőségű n csúcsú gráf, melynek éleinek száma legalább $cn^{4/3}$.*

Bizonyítás. Bizonyítása megtalálható de Caen és Székely [3] cikkében. □

5.8. Lemma. *Jelölje $N_i(x)$ az olyan $n \leq x$ pozitív egész számok számát, melyek prímosztóinak száma (multiplicitással számolva) legfeljebb i. Minden $\delta > 0$ számhoz létezik olyan $C = C(\delta)$ konstans, mellyel tetszőleges $1 \leq i \leq (1-\delta)\log\log x$ esetén teljesül az*

$$N_i(x) < C(\delta) \cdot \frac{x}{\log x} \cdot \frac{(\log\log x)^{i-1}}{(i-1)!}$$

egyenlőtlenség.

Bizonyítás. Jelölje $\pi_i(x)$ az olyan $n \leq x$ pozitív egész számok számát, melyek prímosztóinak száma (multiplicitással számolva) pontosan i. Landau [23] igazolta, hogy tetszőleges $\eta > 0$ esetén létezik olyan $D = D(\delta)$ konstans, mellyel minden $1 \leq i \leq (1-\eta)\log\log x$ számra teljesül az

$$N_i(x) < D(\eta) \cdot \frac{x}{\log x} \cdot \frac{(\log\log x)^{i-1}}{(i-1)!}$$

egyenlőtlenség. Legyen $\delta > 0$ tetszőleges, és legyen $1 \leq i \leq (1-\delta)\log\log x$. Landau eredményét használva felső becslést adunk $N_i(x)$-re:

$$N_i(x) = \sum_{j=0}^{i} \pi_j(x) \leq \sum_{j=0}^{i} D(1+\delta) \cdot \frac{x}{\log x} \cdot \frac{(\log\log x)^{j-1}}{(j-1)!} =$$

$$= D(1+\delta) \cdot \frac{x}{\log x} \cdot \frac{(\log\log x)^{i-1}}{(i-1)!} \sum_{j=0}^{i} \frac{(j-1)(j-2)\dots i}{(\log\log x)^{i-j}} \leq$$

$$\leq D(1+\delta) \cdot \frac{x}{\log x} \cdot \frac{(\log\log x)^{i-1}}{(i-1)!} \sum_{j=0}^{i} \frac{1}{2^{j-i}} \leq 2D(1+\delta) \cdot \frac{x}{\log x} \cdot \frac{(\log\log x)^{i-1}}{(i-1)!},$$

vagyis a $C(\delta) = 2D(1+\delta)$ konstanssal teljesül az igazolni kívánt egyenlőtlenség. ∎

5.9. Lemma. *Legyen $n \in \mathbb{N}$. Minden $m \leq n$ pozitív egész szám felírható*

$$m = uv, \ v \leq u$$

alakban, ahol $u \leq n^{2/3}$, vagy u prímszám.

Bizonyítás. Bizonyítása megtalálható Erdős [9] cikkében. □

5.10. Lemma. *Legyen n pozitív egész szám, valamint legyen* $1 < g$ *tetszőleges valós szám. Minden* $m \leq n$ *pozitív egész szám felírható*

$$m = uv, \ (u, v \in \mathbb{N})$$

alakban, ahol a következő feltételek valamelyike teljesül:

(a) $v \leq u \leq \sqrt{n} \cdot g$,

(b) $\sqrt{n} \cdot g(n) < u$ *olyan, amelyre* $\Omega(u) \leq \frac{\log n}{2 \log g}$.

Továbbá, ha az m számnak nincsen $n^{2/3}$*-nál nagyobb prímosztója, akkor a (b) feltétel helyett a következő feltétellel is teljesül a lemma állítása:*

(b') $n^{1/3} < u \leq n^{2/3}$ *olyan, amelyre* $\Omega(u) \leq \frac{\log n}{2 \log g}$.

Bizonyítás. Legyen az m szám prímtényezős felbontása

$$m = q_1 q_2 \dots q_r, \text{ ahol } q_1 \geq q_2 \geq \dots \geq q_r.$$

A prímtényezőket q_1-től kezdve két részre szétosztva képezzünk két szorzatot úgy, hogy a következő prímet mindig ahhoz a szorzathoz vegyük hozzá, amelyik kisebb. Tehát először q_1 alkotja az egyik szorzatot, a másik (üres) szorzat értéke 1. Következő lépésben q_2 lesz a másik szorzat, $q_1 \geq q_2$ miatt ezután q_3-at is a q_2-t tartalmazó szorzathoz vesszük hozzá - így a két szorzat q_1, illetve $q_2 q_3$ lesz -, majd fent leírt módon folytatjuk a prímtényezők szétosztását. Tegyük fel, hogy i a legkisebb olyan index, hogy a q_i prímtényező hozzávételével már $\sqrt{n} \cdot g$-nél nagyobb lenne az egyik szorzat. A $q_1, \dots, q_{i-1}$ prímeket még két részre lehetett osztani úgy, hogy mindkét részben legfeljebb $\sqrt{n} \cdot g$ a szorzat. Legyen ez a két szorzat A és B, ekkor teljesül az

$$A \leq B \leq \sqrt{n} \cdot g$$

egyenlőtlenség. Tudjuk, hogy $Aq_i > \sqrt{n} \cdot g$, azaz $A > \dfrac{\sqrt{n} \cdot g}{q_i}$. Mivel

$$A^2 \leq AB \leq \frac{m}{q_i} \leq \frac{n}{q_i},$$

ezért

$$\frac{n \cdot g^2}{q_i^2} < A^2 \leq \frac{n}{q_i}$$

miatt $q_i > g^2$. Mivel q_i az i-edik legnagyobb prímosztó, ezért

$$n \geq m \geq q_1 q_2 \dots q_i \geq g^{2i},$$

és így

$$i \leq \frac{\log n}{2 \log g}.$$

A lemma második felének igazolásához feltehetjük, hogy $A \leq n^{1/3}$ és $Aq_i > n^{2/3}$ egyenlőtlenségek teljesülnek, különben $u = A$ vagy $u = Aq_i$ megfelelő választás lenne. Ekkor viszont $q_i > n^{1/3}$ biztosan teljesül, így i értéke csak 1, vagy 2 lehet. Mivel $A \leq B$, ezért $A = 1$, vagyis $Aq_i > n^{2/3}$ egyenlőtlenségből következik, hogy $q_i > n^{2/3}$ az n szám legnagyobb prímosztója, vagyis $i = 1$ és $q_1 > n^{2/3}$ teljesül. Ezzel a lemmát igazoltuk. □

5.2. Az $s_1 s_2 s_3 = t_1 t_2 t_3$ egyenlet

Ebben a fejezetben alsó és felső becslést adunk $G_3(n)$-re.

5.11. Tétel. *Legyen $\varepsilon > 0$ tetszőleges. Ekkor létezik olyan $c > 0$ konstans és $N = N(\varepsilon)$, hogy ha $n > N = N(\varepsilon)$, akkor*

$$\pi(n) + \pi(n/2) + cn^{2/3}/(\log n)^{4/3} \leq G_3(n) \leq$$
$$\leq \pi(n) + \pi(n/2) + \left(\frac{2e}{3} + \varepsilon\right) \cdot n^{2/3} \cdot \frac{\log n}{\log \log n}.$$

Bizonyítás. Először az alsó becslést igazoljuk. Az 5.7. Lemma szerint létezik olyan G gráf, melynek csúcsai a $\sqrt{n}$-nél nem nagyobb páratlan prímszámok, és teljesül, hogy G-ben minden kör hossza legalább 8, valamint G éleinek számára $e(G) \geq c(\pi(\sqrt{n}))^{4/3}$ teljesül. Tekintsük a következő halmazt:

$$A = \{p \mid \sqrt{n} < p \leq n, p \text{ prím}\} \cup \{2q \mid \sqrt{n} < q \leq n/2, q \text{ prím}\} \cup$$
$$\cup \{uv \mid uv \in E(G)\}.$$

Világos, hogy $A \subseteq \{1, 2, \dots, n\}$. Megmutatjuk, hogy az A halmazban az

$$s_1 s_2 s_3 = t_1 t_2 t_3 \ (s_1, s_2, s_3, t_1, t_2, t_3 \in A) \tag{5.1}$$

egyenletnek nincsen páronként különböző elemekből álló megoldása. A G gráf uv élét és az uv szorzatot azonosítjuk. Ezt megtehetjük, mert különböző élekhez különböző szorzatok tartoznak. Először vizsgáljuk azt az esetet, amikor az egyenlet tényezői között szerepel G egy éle. Feltehető, hogy $s_1 = uv \in E(G)$. Ilyenkor v prímszám, ezért v a másik oldalt is osztja. Feltehető, hogy $t_1 = vw \in E(G)$, ahol $w \neq u$, különben $s_1 = t_1$ lenne. Most w osztja az egyenlet bal oldalát, de s_1-et nem, így feltehető, hogy $s_2 = wz \in E(G)$. Ezt folytatva egy legfeljebb 6 hosszú kört kapnánk, ami ellentmondás. Tehát ha az $s_1s_2s_3 = t_1t_2t_3$ egyenletnek lenne megoldása, akkor ebben csak $\sqrt{n}$-nél nagyobb prímek, és ezek kétszeresei szerepelhetnének. Ily módon a hat szám közül pontosan háromnak lenne osztója a 2, ami lehetetlen. Az A halmaz elemszámára fennáll, hogy

$$|A| \geq \pi(n) - \pi(\sqrt{n}) + \pi(n/2) - \pi(\sqrt{n}) + c(\pi(\sqrt{n}))^{3/2} \geq$$
$$\geq \pi(n) + \pi(n/2) + cn^{2/3}/(\log n)^{4/3}.$$

Tegyük fel, hogy az $A \subseteq \{1, 2, \ldots, n\}$ halmazra teljesül, hogy az (5.1) egyenletnek nincsen páronként különböző számokból álló megoldása.

A bizonyításban először az 5.10. Lemmát fogjuk alkalmazni a $g(n) = e^{\frac{\log n}{\log\log n}}$ függvényre. Azért választjuk a $g(n)$ függvényt ilyen nagyságrendűnek, hogy később a (ii) esetnél alkalmazható legyen az 5.8. Lemma. Legyen

$$A = \{a_1, \ldots, a_k\}, \text{ ahol } 1 \leq a_1 < a_2 < \cdots < a_k \leq n.$$

Az 5.10. Lemmát n-re és $g = g(n)$-re alkalmazva azt kapjuk, hogy az A halmaz elemei felírhatók

$$a_i = u_i v_i$$

alakban, ahol u_i és v_i pozitív egész számok, valamint a következő feltételek valamelyike teljesül:

(i) $n^{2/3} < u_i$ prímszám,

(ii) $n^{1/3} < u_i \leq n^{2/3}$ és $\Omega(u_i) \leq \frac{\log n}{2\log g(n)}$,

(iii) $v_i \leq u_i \leq \sqrt{n} \cdot g(n)$.

Ha valamely $1 \leq i \leq k$ esetén több felírás is létezik, akkor válasszuk meg az u_i és v_i számokat úgy, hogy v_i a lehető legkisebb legyen. Az A

halmaz azon elemeinek száma, amelyekre $u_i = v_i$ teljesül felülről becsülhető az $\{1, 2, \dots, n\}$ halmazba eső négyzetszámok számával, így:

$$|\{i \mid 1 \leq i \leq k, u_i = v_i\}| \leq \sqrt{n}. \tag{5.2}$$

Az egyszerűség kedvéért először tegyük fel, hogy A minden elemére fennáll, hogy $u_i \neq v_i$, az így kapott felső becsléshez $\sqrt{n}$-et hozzáadva már tetszőleges A halmazra érvényes felső becslést nyerünk majd. Tegyük fel, hogy az (5.1) egyenletnek nincs olyan megoldása, ahol $s_1, s_2, s_3, t_1, t_2, t_3$ páronként különbözők. Legyen G egy olyan gráf, amelynek csúcsai az $n^{2/3}$-nál nem nagyobb pozitív egész számok kiegészítve az $(n^{2/3}, n]$ intervallumba eső prímekkel:

$$V(G) = \{a \in \mathbb{N} \mid a \leq n^{2/3}\} \cup \{p \mid n^{2/3} < p \leq n, p \text{ prím}\}.$$

A G gráf csúcsainak száma ekkor

$$|V(G)| = \pi(n) + [n^{2/3}] - \pi(n^{2/3}).$$

A G gráf éleit úgy kapjuk, hogy az A halmaz minden elemének megfeleltetünk egy élet: minden $1 \leq i \leq k$ esetén az a_i elemhez tartozó él az u_i és v_i csúcsokat köti össze, ezt az élt a továbbiakban $a_i = u_i v_i$ élnek fogjuk nevezni.

$$E(G) = \{u_i v_i \mid 1 \leq i \leq k\}$$

Ily módon az A halmaz elemeihez különböző éleket rendeltünk, és a kapott G gráfban nincsen hurokél, hiszen elhagytuk azokat az elemeket, amelyekre $u_i = v_i$. A G gráf éleinek száma

$$|E(G)| = |A| = k.$$

Abból, hogy (5.1)-nek nincsen különböző elemekből álló megoldása következik, hogy G nem tartalmaz 6 hosszú kört. Valóban, ha $x_1 x_2 x_3 x_4 x_5 x_6 x_1$ egy 6 hosszú kör lenne G-ben, akkor

$$s_1 = x_1 x_2, t_1 = x_2 x_3, s_2 = x_3 x_4, t_2 = x_4 x_5, s_3 = x_5 x_6, t_3 = x_6 x_1$$

olyan páronként különböző A-beli elemek lennének, amelyek kielégítik az (5.1) egyenletet.

Célunk a G gráf éleinek k számát felülről becsülni. Ehhez G éleit felosztjuk néhány csoportba. Legyen G_0 az a részgráf, amely G azon $u_i v_i$ éleit tartalmazza, amelyekre $\max(u_i, v_i) \leq \sqrt{n}$:

$$E(G_0) = \{u_i v_i \mid u_i \leq \sqrt{n}\}.$$

Legyen K_1 egy pozitív egész szám, melyet később választunk meg, és minden $1 \le h \le K_1$ esetén legyen G_h az a részgráf, amely G azon $u_i v_i$ éleit tartalmazza, amelyekre fennáll a

$$\sqrt{n} \cdot g(n)^{\frac{h-1}{K_1}} < u_i \le \sqrt{n} \cdot g(n)^{\frac{h}{K_1}}$$

egyenlőtlenség:

$$E(G_h) = \{u_i v_i \mid \sqrt{n} \cdot g(n)^{\frac{h-1}{K_1}} < u_i \le \sqrt{n} \cdot g(n)^{\frac{h}{K-1}}\}.$$

A $G_0, G_1, \ldots, G_{K_1}$ gráfok tartalmazzák az összes olyan élet, amelyre (iii) teljesül.

A fennmaradó élek közül azokat, amelyekre (ii) teljesül felosztjuk K_2 csoportba, ahol a K_2 pozitív egész számot később határozzuk meg. Ezekre az $u_i v_i$ élekre $n^{1/3} \le u_i \le n^{2/3}$ és $\Omega(u_i) \le \frac{\log n}{2 \log g(n)}$ teljesül. Legyen tehát $1 \le h \le K_2$ esetén G_{K_1+h} az a részgráf, amely az

$$E(G) \setminus (E(G_0) \cup \cdots \cup E(G_{K_1}))$$

halmazba eső $u_i v_i$ élek közül azokat tartalmazza, amelyekre fennáll az

$$n^{\frac{1}{3}+\frac{h-1}{3K_2}} < u_i \le n^{\frac{1}{3}+\frac{h}{3K_2}}$$

egyenlőtlenség:

$$E(G_h) = \{u_i v_i \mid n^{\frac{1}{3}+\frac{h-1}{3K_2}} \le u_i < n^{\frac{1}{3}+\frac{h}{3K_2}}\} \setminus \cup_{j=0}^{K_1} E(G_j).$$

Ha $u_i v_i \in E(G_h)$, akkor $\Omega(u_i) \le \frac{\log n}{2 \log g(n)}$ is teljesül.

Végül legyen $G_{K_1+K_2+1}$ az a gráf, melyet úgy kapunk meg, hogy a G_0, G_1, ..., $G_{K_1+K_2}$ gráfok éleit töröljük G-ből. A $G_{K_1+K_2+1}$ gráf éleihez tartozó A-beli elemekre $n^{2/3} < u_i$, azaz u_i prímszám, és ezek az élek (i)-et elégítik ki:

$$E(G_{K_1+K_2+1}) = \{u_i v_i \mid n^{2/3} \le u_i,\ u_i \text{ prímszám}\}.$$

Így a G gráfot $K_1 + K_2 + 2$ részre osztottuk fel. Jelöljük k_h-val a G_h gráf éleinek számát ($0 \le h \le K_1 + K_2 + 1$). A bizonyítás további részében külön-külön felülről becsüljük a k_h élszámokat, végül összegezzük a kapott becsléseket.

A G_0 gráfnak legfeljebb $[\sqrt{n}]$ olyan csúcsa van, amelyből indul él, hiszen $u_i v_i \in E(G_0)$ esetén $v_i < u_i \leq \sqrt{n}$. Így az 5.2. Lemma szerint éleinek számára teljesül a

$$k_0 \leq 0,6272(\sqrt{n})^{4/3} = 0,6272n^{2/3} \tag{5.3}$$

egyenlőtlenség, ha n elég nagy.

Legyen most $1 \leq h \leq K_1$. Ha valamely $a_i = u_i v_i$ a G_h gráf éle, akkor

$$\sqrt{n} \cdot g(n)^{\frac{h-1}{K_1}} < u_i \leq \sqrt{n} \cdot g(n)^{\frac{h}{K_1}}$$

és így

$$v_i = \frac{a_i}{u_i} \leq \frac{n}{u_i} \leq \frac{\sqrt{n}}{g(n)^{\frac{h-1}{K_1}}}.$$

Ez azt jelenti, hogy G_h egy olyan páros gráf, ahol a két független csúcsosztályra, U_h-ra és V_h-ra, a következők teljesülnek:

$$U_h \subseteq \left\{ \left[\sqrt{n} \cdot g(n)^{\frac{h-1}{K_1}}\right] + 1, \ldots, \left[\sqrt{n} \cdot g(n)^{\frac{h}{K_1}}\right] \right\},$$

$$V_h \subseteq \left\{ 1, 2, \ldots, \left[\sqrt{n}/g(n)^{\frac{h-1}{K_1}}\right] \right\}.$$

(Azokat a csúcsokat, amelyekből nem indul él, elhagyjuk a G_h gráfból.) Az 5.4. Lemma szerint G_h éleinek számára teljesül a következő egyenlőtlenség:

$$\begin{aligned} k_h &\leq (|U_h||V_h|)^{2/3} + 16(|U_h| + |V_h|) \leq \\ &\leq n^{\frac{2}{3}} g(n)^{\frac{2}{3K_1}} + 16 \left(\left[\sqrt{n} \cdot g(n)^{\frac{h}{K_1}}\right] - \left[\sqrt{n} \cdot g(n)^{\frac{h-1}{K_1}}\right] \right) + \frac{\sqrt{n}}{g(n)^{\frac{h-1}{K_1}}}. \end{aligned}$$

A k_h-ra kapott felső becslést $1 \leq h \leq K_1$ esetén összegezve:

$$\begin{aligned} \sum_{h=1}^{K_1} k_h &\leq K_1 n^{\frac{2}{3}} g(n)^{\frac{2}{3K_1}} + \\ &+ 16 \sum_{h=1}^{K_1} \left(\left[\sqrt{n} \cdot g(n)^{\frac{h}{K_1}}\right] - \left[\sqrt{n} \cdot g(n)^{\frac{h-1}{K_1}}\right] \right) + 16 \sum_{h=1}^{K_1} \frac{\sqrt{n}}{g(n)^{\frac{h-1}{K_1}}} \leq \\ &\leq K_1 n^{\frac{2}{3}} g(n)^{\frac{2}{3K_1}} + 16\sqrt{n} \cdot g(n) + 16 \cdot \frac{1 - \frac{1}{g(n)}}{1 - \frac{1}{g(n)^{1/K_1}}} \cdot \sqrt{n}, \end{aligned} \tag{5.4}$$

hiszen az egyik szumma egy teleszkopikus összeg, a másik pedig egy K_1 tagú mértani sorozat tagjainak összege. Könnyű látni, hogy akkor kapjuk a legjobb becslést, ha K_1 értékét úgy választjuk meg, hogy $K_1 g(n)^{\frac{2}{3K_1}}$ minimális legyen. A $K_1 \to K_1 g(n)^{\frac{2}{3K_1}}$ függvényt megvizsgálva azt kapjuk, hogy a legkisebb értékét $K_1 = \frac{2\log g(n)}{3}$-ra veszi fel, ahol a függvény értéke $\frac{2e}{3} \cdot \log g(n)$. Legyen tehát $K_1 = \left\lceil \frac{2\log g(n)}{3} \right\rceil$, a felső egészrész számunkra elhanyagolható nagyságú hibát okoz:

$$K_1 g(n)^{\frac{2}{3K_1}} < \left(\frac{2\log g(n)}{3} + 1 \right) \cdot g(n)^{1/\log g(n)} = \frac{2e}{3} \cdot \log g(n) + e. \tag{5.5}$$

Mivel $K_1 \le \log g(n)$, ezért

$$16 \cdot \frac{1 - \frac{1}{g(n)}}{1 - \frac{1}{g(n)^{1/K_1}}} \cdot \sqrt{n} \le \frac{16}{1 - 1/e} \cdot \sqrt{n}. \tag{5.6}$$

Tehát (5.4) egyenlőtlenségből $K_1 = \frac{2\log g(n)}{3}$ választással (5.5)-öt és (5.6)-ot figyelembe véve a következő becslést nyerjük:

$$\begin{aligned} \sum_{h=1}^{K_1} k_h \le & \\ & \le \frac{2e}{3} \cdot n^{2/3} \log g(n) + e \cdot n^{2/3} + 16\sqrt{n} \cdot g(n) + \frac{16}{1 - 1/e} \cdot \sqrt{n} \le \\ & \le \frac{2e}{3} \cdot n^{2/3} \cdot \frac{\log n}{\log\log n} + c_1 n^{2/3}, \end{aligned} \tag{5.7}$$

ahol $c_1 > e$ tetszőleges konstans, és n elegendően nagy.

Legyen most $1 \le h \le K_2$. Ha valamely $a_i = u_i v_i$ a G_{K_1+h} gráf éle, akkor

$$n^{\frac{1}{3} + \frac{h-1}{3K_2}} < u_i \le n^{\frac{1}{3} + \frac{h}{3K_2}}$$

és így

$$v_i = \frac{a_i}{u_i} \le \frac{n}{u_i} \le n^{\frac{2}{3} - \frac{h-1}{3K_2}}.$$

Ez azt jelenti, hogy G_h egy olyan páros gráf, ahol a két független csúcsosztályra: U_{K_2+h}-ra és V_{K_2+h}-ra a következők teljesülnek:

$$U_{K_1+h} \subseteq \left\{ \left[n^{\frac{1}{3} + \frac{h-1}{3K_2}} \right] + 1, \ldots, \left[n^{\frac{1}{3} + \frac{h}{3K_2}} \right] \right\},$$

$$V_{K_1+h} \subseteq \left\{1, 2, \ldots, \left[n^{\frac{2}{3}-\frac{h-1}{3K_2}}\right]\right\},$$

valamint azt is tudjuk, hogy U_{K_2+h} minden u_i elemére

$$\Omega(u_i) \leq \frac{\log n}{2 \log g(n)} = \frac{1}{2} \cdot \log \log n$$

is fennáll. (Azokat a csúcsokat, amelyekből nem indul él, elhagyjuk a G_{K_2+h} gráfból.) Legyen $s = \left\lfloor \frac{1}{2} \cdot \log \log n \right\rfloor - 1$. Az 5.8. Lemma szerint létezik olyan c' konstans, amellyel teljesül a következő egyenlőtlenség:

$$N_{s+1}(x) \leq c' \cdot \frac{x}{\log x} \cdot \frac{(\log \log x)^s}{s!},$$

ahol $N_{s+1}(x)$-szel az x-nél nem nagyobb, legfeljebb $s+1$ prím szorzataként felírható számok számát jelöljük:

$$N_{s+1}(x) = |\{a \in \mathbb{N} \mid a \leq x \text{ és } \Omega(a) \leq s+1\}|.$$

Az összefüggést $x = n^{\frac{1}{3}+\frac{h}{3K_2}}$-re alkalmazva kapjuk, hogy

$$\begin{aligned} |U_{K_1+h}| \leq N_s(n^{\frac{1}{3}+\frac{h}{3K_2}}) \leq \\ \leq c' \cdot \frac{n^{\frac{1}{3}+\frac{h}{3K_2}}}{(\frac{1}{3}+\frac{h}{3K_2}) \log n} \cdot \frac{\left(\log \log n^{\frac{1}{3}+\frac{h}{3K_2}}\right)^s}{s!} \leq \\ \leq 3c' \cdot \frac{n^{\frac{1}{3}+\frac{h}{3K_2}}}{\log n} \cdot \frac{(\log \log n)^s}{s!}. \end{aligned} \tag{5.8}$$

A kapott kifejezés becsléséhez $\frac{\log \log n}{s}$ értékét becsüljük meg. Legyen $\eta > 0$ tetszőleges. Ha n elegendően nagy, akkor teljesül, hogy

$$\frac{\log \log n}{s} = \frac{\log \log n}{\left\lfloor \frac{1}{2} \cdot \log \log n \right\rfloor - 1} \leq 2 + \eta.$$

Ezt és az $s! \geq (s/e)^s$ összefüggést felhasználva

$$\begin{aligned} \frac{(\log \log n)^s}{s!} \leq \frac{(\log \log n)^s}{(s/e)^s} = ((2+\eta)e)^{\frac{1}{2} \log \log n} = \\ = (\log n)^{\frac{1}{2} \log((2+\eta)e)} < (\log n)^{9/10}, \end{aligned}$$

ha $0 < \eta$-t elegendően kicsinek választjuk, ugyanis $\eta = 0$ esetén $\log n$ kitevőjének értéke kisebb, mint 0,9. Ezt (5.8)-ba visszaírva

$$|U_{K_1+h}| \le 3c' \cdot \frac{n^{\frac{1}{3}+\frac{h}{3K_2}}}{(\log n)^{1/10}}$$

adódik. Továbbá világos, hogy

$$|V_{K_1+h}| \le n^{\frac{2}{3}-\frac{h-1}{3K_2}}.$$

Az 5.4. Lemma szerint G_{K_1+h} éleinek számára teljesül a következő egyenlőtlenség:

$$\begin{aligned} k_{K_1+h} &\le (|U_{K_1+h}||V_{K_1+h}|)^{2/3} + 16(|U_{K_1+h}| + |V_{K_1+h}|) \le \\ &\le n^{\frac{2}{3}+\frac{2}{9K_2}}/(\log n)^{1/15} + 16\left(3c' \cdot \frac{n^{\frac{1}{3}+\frac{h}{3K_2}}}{(\log n)^{1/10}} + n^{\frac{2}{3}-\frac{h-1}{3K_2}}\right). \end{aligned}$$

A k_h-ra kapott felső becslést $1 \le h \le K_2$ esetén összegezve:

$$\begin{aligned} \sum_{h=1}^{K_2} k_{K_1+h} \le K_2 n^{\frac{2}{3}+\frac{2}{9K_2}}/(\log n)^{1/15} + \\ + 16\sum_{h=1}^{K_2}\left(3c' \cdot \frac{n^{\frac{1}{3}+\frac{h}{3K_2}}}{(\log n)^{1/10}} + n^{\frac{2}{3}-\frac{h-1}{3K_2}}\right), \end{aligned} \tag{5.9}$$

ebben a kifejezésben a második összegben kétszer is megjelenő $n^{\frac{1}{3}+\frac{h}{3K_2}}$ $(1 \le h \le K_2)$ mértani sorozatot összegezve:

$$\left(\frac{48c'}{\log n} + 16\right) \cdot \sum_{h=1}^{K_2} n^{\frac{1}{3}+\frac{h}{3K_2}} = \left(\frac{48c'}{\log n} + 16\right) \cdot \frac{n^{\frac{2}{3}+\frac{1}{3K_2}} - n^{\frac{1}{3}+\frac{1}{3K_2}}}{n^{\frac{1}{3K_2}} - 1}. \tag{5.10}$$

A (5.9) becslésben $K_2 n^{\frac{2}{3}+\frac{2}{9K_2}}/(\log n)^{1/15}$ a legnagyobb tag. Úgy érdemes K_2 értékét megválasztani, hogy $K_2 n^{\frac{2}{9K_2}}$ minimális legyen. A $K_2 \to K_2 n^{\frac{2}{9K_2}}$ függvényt megvizsgálva azt kapjuk, hogy a legkisebb értékét $K_2 = \frac{2\log n}{9}$-re veszi fel, ahol a függvény értéke $\frac{2e\log n}{9}$. Legyen tehát $K_2 = \left\lceil \frac{2\log n}{9} \right\rceil$, a felső egészrész számunkra elhanyagolható nagyságú hibát okoz:

$$K_2 n^{\frac{2}{9K_2}} < \left(\frac{2\log n}{9} + 1\right) n^{\frac{2}{9K_2}} = \frac{2e\log n}{9} + e.$$

A K_2 értékét így választva meg (5.10) értéke:

$$\left(\frac{48c'}{\log n}+16\right)\cdot\frac{n^{\frac{2}{3}+\frac{1}{3K_2}}-n^{\frac{1}{3}+\frac{1}{3K_2}}}{n^{\frac{1}{3K_2}}-1}\le c_2\cdot n^{2/3},$$

ahol $c_2>\left(\frac{48c'}{\log n}+16\right)\cdot\frac{e^{3/2}}{e^{3/2}-1}$ tetszőleges konstans. Ezzel a választással (5.9) egyenlőtlenségből azt kapjuk, hogy

$$\sum_{h=1}^{K_2}k_{K_1+h}\le\frac{2e}{9}n^{2/3}(\log n)^{9/10}+c_3\cdot n^{2/3},\tag{5.11}$$

ahol $c_3=c_2+e$.

Végül, $G_{K_1+K_2+1}$ szintén páros gráf, az $(n^{2/3},n]$ halmazba eső prímek, illetve az $n^{1/3}$-nál kisebb pozitív egészek alkotják a két független csúcsosztályt. (A 0 fokú csúcsokat ismét elhagyjuk.) Ha $p\in(n/2,n]$, akkor a p-nek megfelelő csúcsból legfeljebb egy él indulhat, a $p\cdot 1$-nek megfelelő, hiszen $2p>n$ miatt p nem lehet összekötve 1-nél nagyobb egész számmal. Hagyjuk el az $1p$ éleket és p csúcsokat $G_{K_1+K_2+1}$-ből, a megmaradó gráf legyen $G'_{K_1+K_2+1}$. Az elhagyott élek száma legfeljebb $\pi(n)-\pi(n/2)$. A $G'_{K_1+K_2+1}$ gráf sem tartalmaz 6 hosszú kört, és minden éle egy $(n^{2/3},n/2]$-be eső prímszámot köt össze egy $n^{1/3}$-nál kisebb pozitív egész számmal. Tehát egy olyan páros gráf, amelynek R és S független csúcsosztályaira fennáll, hogy

$$R\subseteq\{p\mid n^{2/3}<p\le n/2, p\text{ prím}\},\text{ illetve}$$

$$S\subseteq\{a\in\mathbb{N}\mid a<n^{1/3}\}.$$

(Azokat a csúcsokat, amelyekből nem indul él, elhagyjuk a gráfból.) Az 5.5. Lemma szerint $G'_{K_1+K_2+1}$ éleinek számára

$$k'_{K_1+K_2+1}\le 2|R|+|S|^2/2\le 2(\pi(n/2)-\pi(n^{2/3}))+n^{2/3}/2$$

teljesül. Ezért

$$k_{K_1+K_2+1}\le\pi(n)-\pi(n/2)+k'_{K_1+K_2+1}\le\pi(n)+\pi(n/2)+n^{2/3}/2.\tag{5.12}$$

Adjuk össze az (5.3), (5.7), (5.11), (5.12) egyenlőtlenségeket:

$$k = \sum_{h=0}^{K_1+K_2+1} k_h \leq 0,6272n^{2/3} + \frac{2e}{3} \cdot n^{2/3} \cdot \frac{\log n}{\log \log n} + c_1 n^{2/3} +$$
$$+ \frac{2e}{9} n^{2/3} (\log n)^{9/10} + c_3 \cdot n^{2/3} + \pi(n) + \pi(n/2) + n^{2/3}/2 \leq$$
$$\leq \pi(n) + \pi(n/2) + \left(\frac{2e}{3} + \varepsilon \right) \cdot n^{2/3} \cdot \frac{\log n}{\log \log n},$$

ahol $\varepsilon > 0$ tetszőleges, és n elegendően nagy. A négyzetszámok elhagyásából származó hiba (5.2) egyenlőtlenség szerint $O(n^{1/2})$, így a kapott becslés tetszőleges A halmazra fennáll, amennyiben n elég nagy. Ezzel igazoltuk a tétel állítását.

□

5.3. Az $s_1 s_2 s_3 s_4 = t_1 t_2 t_3 t_4$ egyenlet

A következő tétel nem csak $G_4(n)$-re ad felső becslést, hanem tetszőleges $k \geq 2$ mellett $G_{2k}(n)$-re is.

5.12. Tétel. *Tetszőleges $k \geq 2$ és tetszőleges $\varepsilon > 0$ esetén létezik olyan $N = N(k, \varepsilon)$, hogy ha $n > N$, akkor*

$$G_{2k}(n) \leq \pi(n) + (c + \varepsilon) n^{2/3},$$

ahol $k = 2$ esetén $c = 10$, $k = 3$ esetén $c = 6$, $k > 3$ esetén pedig $c = 2k - 3$.

Bizonyítás. Legyen

$$A = \{a_1, \dots, a_k\}, \text{ ahol } 1 \leq a_1 < a_2 < \dots < a_k \leq n.$$

Tegyük fel, hogy A-ban nincs megoldása az

$$s_1 s_2 \dots s_{2k} = t_1 t_2 \dots t_{2k} \ (s_1, \dots, s_{2k}, t_1, \dots, t_{2k} \in A) \tag{5.13}$$

egyenletnek. Az 5.9. Lemmát n-re alkalmazva azt kapjuk, hogy az A halmaz elemei felírhatók

$$a_i = u_i v_i$$

alakban, ahol u_i és v_i pozitív egész számok, valamint a következő feltételek valamelyike teljesül:

(i) $n^{2/3} < u_i$ prímszám,

(ii) $v_i \leq u_i \leq n^{2/3}$.

Ha valamely $1 \leq i \leq k$ esetén több felírás is létezik, akkor válasszuk meg az u_i és v_i számokat úgy, hogy v_i a lehető legkisebb legyen. Az A halmaz azon elemeinek száma, amelyekre $u_i = v_i$ teljesül felülről becsülhető az $\{1, 2, \ldots, n\}$ halmazba eső négyzetszámok számával, így:

$$|\{i \mid 1 \leq i \leq k, u_i = v_i\}| \leq \sqrt{n}. \tag{5.14}$$

Az egyszerűség kedvéért először tegyük fel, hogy A minden elemére $u_i \neq v_i$ teljesül, az így kapott felső becsléshez $\sqrt{n}$-et hozzáadva már tetszőleges A halmazra érvényes felső becslést nyerünk majd. Tegyük fel, hogy az (5.13) egyenletnek nincs olyan megoldása, ahol $s_1, \ldots, s_{2k}$, $t_1, \ldots, t_{2k}$ páronként különbözők. Legyen G egy olyan gráf, amelynek csúcsai az $n^{2/3}$-nál nem nagyobb pozitív egész számok kiegészítve az $(n^{2/3}, n]$ intervallumba eső prímekkel:

$$V(G) = \{a \in \mathbb{N} \mid a \leq n^{2/3}\} \cup \{p \mid n^{2/3} < p \leq n,\ p \text{ prím}\}.$$

A G gráf csúcsainak száma

$$|V(G)| = \pi(n) + [n^{2/3}] - \pi(n^{2/3}).$$

Az A halmaz minden elemének megfeleltetünk egy élet: minden $1 \leq i \leq k$ esetén az a_i elemhez tartozó él az u_i és v_i csúcsokat köti össze, ezt az élt a továbbiakban $a_i = u_i v_i$ élnek fogjuk nevezni.

$$E(G) = \{u_i v_i \mid 1 \leq i \leq k\}$$

Ily módon az A halmaz elemeihez különböző éleket rendeltünk, a kapott G gráfban nincsen hurokél, hiszen elhagytuk azokat az elemeket, amelyekre $u_i = v_i$. A G gráf éleinek száma

$$|E(G)| = |A| = k.$$

Abból, hogy (5.13)-nak nincsen különböző elemekből álló megoldása következik, hogy a G gráf nem tartalmaz $4k$ hosszú kört. Valóban, ha $x_1 x_2 \ldots x_{4k} x_1$ egy $4k$ hosszú kör lenne G-ben, akkor

$$s_i = x_{2i-1} x_{2i},\ t_i = x_{2i} x_{2i+1}\ (1 \leq i \leq 2k)$$

számok (ahol $x_{4k+1} := x_1$) olyan páronként különböző A-beli elemek lennének, amelyek kielégítik az (5.13) egyenletet.

Célunk a G gráf éleinek k számát felülről becsülni. Ehhez G éleit felosztjuk néhány csoportba. Legyen G_0 az a részgráf, amely G azon $u_i v_i$ éleit tartalmazza, amelyekre $v_i \leq u_i \leq \sqrt{n}$ teljesül:

$$E(G_0) = \{u_i v_i \mid u_i \leq \sqrt{n}\}.$$

Legyen G_1 az a részgráf, amely azon $u_i v_i$ éleket tartalmazza, amelyekre $\sqrt{n} < u_i \leq n^{2/3}$. A $k = 2$ esetben ahhoz, hogy elegendően pontos becsléseket kapjunk, szükséges lesz a G_1 gráf éleinek további osztályokra bontása. Legyen G_1', illetve G_1'' az a részgráf, amely G_1 azon $u_i v_i$ éleit tartalmazza, amelyekre $\sqrt{n} < u_i \leq n^{7/12}$, illetve $n^{7/12} < u_i \leq n^{2/3}$:

$$E(G_1') = \{u_i v_i \mid \sqrt{n} < u_i \leq n^{7/12}\},$$

$$E(G_1'') = \{u_i v_i \mid n^{7/12} < u_i \leq n^{2/3}\}.$$

A G_0, G_1 gráfok tartalmazzák az összes olyan élet, amelyre (ii) teljesül.

Legyen G_2 az a gráf, melyet úgy kapunk, hogy a G_0, G_1 gráfok éleit töröljük G-ből. A G_2 gráf éleihez tartozó A-beli elemekre $n^{2/3} < u_i$, azaz u_i prímszám, és ezek az élek (i)-et elégítik ki:

$$E(G_2) = \{u_i v_i \mid n^{2/3} \leq u_i,\ u_i \text{ prímszám}\}.$$

Így a G gráfot 3 részre osztottuk fel. Jelöljük k_h-val a G_h gráf éleinek számát ($0 \leq h \leq 2$). A bizonyítás további részében külön-külön felülről becsüljük a k_h élszámokat, végül összegezzük a kapott becsléseket.

A G_0 gráfnak legfeljebb $[\sqrt{n}]$ olyan csúcsa van, amelyből indul él, hiszen $u_i v_i \in E(G_0)$ esetén $v_i < u_i \leq \sqrt{n}$. Így az 5.3. Lemma szerint éleinek számára teljesül a

$$k_0 \leq 200k \cdot n^{\frac{1}{2}+\frac{1}{4k}} \tag{5.15}$$

egyenlőtlenség.

Ha $u_i v_i$ éle a G_1 gráfnak, akkor

$$v_i = \frac{n}{u_i} \leq \frac{n}{\sqrt{n}} = \sqrt{n}.$$

Ez azt jelenti, hogy a G_1 páros gráf független csúcsosztályainak elemszáma legfeljebb $n^{2/3}$, illetve $n^{1/2}$. Az 5.6. Lemma szerint G_1 gráf élszámára a következő felső becslés érvényes:

$$k_1 \le (2k-3)(n^{\frac{2}{3}\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{2k+2}{4k}} + n^{\frac{2}{3}} + n^{\frac{1}{2}}) = \\ = (2k-3)n^{\frac{1}{3}+\frac{k+1}{4k}} + (2k-3)n^{2/3} + (2k-3)n^{1/2}. \quad (5.16)$$

A $k = 2$ esetben ez a becslés túlságosan pontatlan, ezért ebben az esetben G_1' és G_1'' élszámára külön-külön adunk becslést az 5.6. Lemmát használva az előzőekhez hasonlóan:

$$k_1' \le 5(n^{\frac{7}{12}\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{3}{4}} + n^{\frac{7}{12}} + n^{\frac{1}{2}}) = 5n^{2/3} + 5n^{7/12} + 5n^{1/2},$$

$$k_1'' \le 5(n^{\frac{2}{3}\cdot\frac{1}{2}+\frac{5}{12}\cdot\frac{3}{4}} + n^{\frac{2}{3}} + n^{\frac{5}{12}}) = 5n^{2/3} + 5n^{31/48} + 5n^{5/12}.$$

Itt k_1'' becslésénél kihasználtuk, hogy ha u_iv_i éle G_1''-nek, akkor $v_i \le n/u_i \le n^{5/12}$. Így azt kapjuk, hogy $k = 2$ esetén a G_1 gráf éleinek számára fennáll a következő egyenlőtlenség:

$$k_1 = k_1' + k_1'' \le 10n^{2/3} + 5n^{7/12} + 5n^{1/2} + 5n^{31/48} + 5n^{5/12}. \quad (5.17)$$

Végül, G_2 szintén páros gráf, az $(n^{2/3}, n]$ halmazba eső prímek, illetve az $n^{1/3}$-nál kisebb pozitív egészek alkotják a két független csúcsosztályt. (A 0 fokú csúcsokat ismét elhagyjuk.) Tehát G_2 egy olyan páros gráf, amelynek R és S független csúcsosztályaira fennáll, hogy

$$R \subseteq \{p \mid n^{2/3} < p \le n,\ p \text{ prím}\},\ \text{illetve}$$

$$S \subseteq \{a \in \mathbb{N} \mid a < n^{1/3}\}.$$

(Azokat a csúcsokat, amelyekből nem indul él, elhagyjuk a gráfból.) A G_2 gráf nem tartalmazhat $4k$ hosszú kört, és megmutatjuk, hogy k páronként éldiszjunkt 4 hosszú kört sem. Tegyük fel ugyanis, hogy $y_{i,1}y_{i,2}y_{i,3}y_{i,4}y_{i,1}$ $(1 \le i \le k\ )$ éldiszjunkt 4 hosszú körök G_2-ben. Ekkor az $y_{i,1}y_{i,2}$ és $y_{i,3}y_{i,4}$ számok szorzata megegyezne az $y_{i,2}y_{i,3}$ és $y_{i,4}y_{i,1}$ számok szorzatával minden $1 \le i \le k$ esetén, és így lenne páronként különböző A-beli elemekből álló megoldása az $s_1 \ldots s_{2k} = t_1 \ldots t_{2k}$ egyenletnek. Vagyis G_2 nem tartalmazhat k páronként éldiszjunkt 4 hosszú kört, és így legfeljebb $4(k-1)$ él törlésével elérhető, hogy egyetlen 4 hosszú kört se tartalmazzon (ha tartalmaz 4 hosszú kört, töröljük az egyik ilyen kör összes élét, ha még mindig tartalmaz, ismét töröljük, végül, legkésőbb a $(k-1)$-edik kör éleinek törlése után a megmaradó részgráfban már nem lehet újabb 4 hosszú kör). Jelölje G_2' az így kapott gráfot, éleinek számára $k_2' \geq k_2 - 4(k-1)$ áll fenn.

Definiálunk S-en egy H gráfot. A következő módon kapjuk H éleit. Sorra vesszük R pontjait, és minden $v \in R$ csúcs G_2'-beli szomszédjainak berajzoljuk egy maximális párosítását H-ban. Ha v foka 0, vagy 1, akkor nem keletkezik él, ha v foka páros, akkor $d(v)/2$, ha v foka páratlan, akkor $(d(v)-1)/2$ élt rajzolunk be. Vegyük észre, hogy ha H-ban ab él, akkor ezt az élt az a és b csúcsok közös G_2'-beli szomszédjánál húztuk be. Ez a közös szomszéd egyértelmű, ellenkező esetben G_2' tartalmazna 4 hosszú kört. Tehát az eljárás során különböző R-beli csúcsok esetén különböző éleket húztunk be. Ha $d(v) \geq 2$, akkor $d(v)/3 \leq \lfloor d(v)/2 \rfloor$, azaz H éleinek száma legalább 1/3-szorosa G_2' olyan élei számának, melyek R-beli végpontja nem elsőfokú. Ez azt jelenti, hogy

$$k_2' \leq |R| + 3k_H,$$

ahol k_H jelöli H éleinek számát. Megmutatjuk, hogy H nem tartalmaz $2k$ hosszú kört. Tegyük fel ugyanis, hogy $u_1u_2 \dots u_{2k}u_1$ egy kör H-ban. Ekkor H definíciója miatt vannak olyan $v_1, v_2, \dots, v_{2k} \in R$ csúcsok, amelyekre $u_1v_1u_2v_2 \dots u_{2k}v_{2k}u_1$ egy $4k$ hosszú kör lenne G_2'-ben. Tehát H egy olyan C_{2k}-mentes gráf, melynek $[n^{1/3}]$ csúcsa van, így az 5.3. Lemma szerint éleinek számára teljesül, hogy

$$k_H \leq (100k)n^{\frac{1}{3}\left(1+\frac{1}{k}\right)}.$$

Ezért

$$k_2 \leq |R| + 3k_H + 4(k-1) \leq \pi(n) + (300k)n^{\frac{1}{3}\left(1+\frac{1}{k}\right)} + 4(k-1). \tag{5.18}$$

Összefoglalva a kapott eredményeket, vagyis az (5.15), (5.16), (5.18) egyenlőtlenségeket összeadva:

$$\begin{aligned} k = k_0 + k_1 + k_2 \leq (200k \cdot n^{\frac{1}{2}+\frac{1}{4k}}) + ((2k-3)n^{\frac{1}{3}+\frac{k+1}{4k}} + (2k-3)n^{2/3} + \\ + (2k-3)n^{1/2}) + (\pi(n) + (300k)n^{\frac{1}{3}\left(1+\frac{1}{k}\right)} + 4(k-1)) \leq \\ \leq \pi(n) + (2k-3+\varepsilon)n^{2/3} \end{aligned}$$

teljesül $k \geq 4$ esetén, ha $\varepsilon > 0$ és n elegendően nagy. Ha $k = 3$, akkor pedig $k \leq \pi(n) + (6+\varepsilon)n^{2/3}$ felső becslést kapjuk. Ha $k = 2$, akkor k_1 becslésére

(5.17) egyenlőtlenséget használva a következő becslést kapjuk:

$$k = k_0 + k_1 + k_2 \leq (400 \cdot n^{\frac{1}{2}+\frac{1}{8}}) + (10n^{2/3} + 5n^{7/12} + 5n^{1/2} + 5n^{31/48} + 5n^{5/12}) + (\pi(n) + (300 \cdot 2)n^{\frac{1}{3}\left(1+\frac{1}{2}\right)}) \leq \leq \pi(n) + (10 + \varepsilon)n^{2/3},$$

ahol $\varepsilon > 0$ és n elegendően nagy. Ezek a felső becslések tetszőleges A halmazra érvényesek, mert (5.14) elhanyagolható nagyságú hibát okoz. Ezzel bizonyítottuk az állítást. □

Most alsó becslést adunk $G_4(n)$-re.

5.13. Tétel. *Ha n elegendően nagy, akkor fennáll a*

$$G_4(n) \geq \pi(n) + n^{3/5}/(\log n)^{6/5}$$

egyenlőtlenség.

Bizonyítás. Legyen $n \in \mathbb{N}$ és legyen

$$S = \{p \mid p \leq n^{2/5}(\log n)^{1/5},\ p \text{ prím}\},$$

$$T = \{p \mid n^{2/5}(\log n)^{1/5} < p \leq n,\ p \text{ prím}\}.$$

Először konstruálunk egy G_0 páros gráfot, melyben a két független csúcsosztály S és T, így a csúcsok halmaza:

$$V(G_0) = S \cup T.$$

Ehhez vegyünk egy C_4-mentes H gráfot S-en, melynek éleinek számára

$$\frac{1}{3}\pi(n^{2/5}(\log n)^{1/5})^{3/2} \leq e(H) \leq \frac{2}{5}\pi(n^{2/5}(\log n)^{1/5})^{3/2}.$$

Ilyen létezik az 5.1. Lemma szerint. A H gráf éleinek injektív módon megfeleltetjük T olyan csúcsait, melyek az $\left(n^{2/5}(\log n)^{1/5}, n^{3/5}/(\log n)^{1/5}\right]$ intervallumba esnek. Ezt megtehetjük, ugyanis

$$\left|T \cap \left(n^{2/5}(\log n)^{1/5}, n^{3/5}/(\log n)^{1/5}\right]\right| = = \pi(n^{3/5}/(\log n)^{1/5}) - \pi(n^{2/5}(\log n)^{1/5}) \geq \frac{2}{5}\pi(n^{2/5}(\log n)^{1/5})^{3/2},$$

ha n elegendően nagy. Amennyiben az $uv \in E(H)$ élnek a $w \in T$ csúcsot feleltettük meg, cseréljük le az uv élt az uwv cseresznyére. Különböző uv élekhez különböző $w \in T$ csúcs tartozik, továbbá $uw \leq n$ és $vw \leq n$ egyenlőtlenségek teljesülnek, hiszen $u, v \leq n^{2/5}(\log n)^{1/5}$ és $w \leq n^{3/5}/(\log n)^{1/5}$. A kapott páros gráf legyen G_0. A G_0 gráfban két S-beli csúcsnak legfeljebb egy közös szomszédja van, és pontosan akkor van közös szomszédjuk, ha H-ban futott köztük él. A G_0 gráf éleinek száma

$$|E(G_0)| = 2|E(H)| \geq \frac{2}{3}\pi(n^{2/5}(\log n)^{1/5})^{3/2}.$$

Azt állítjuk, hogy G_0-ban nincsen sem 4, sem 8 hosszú kör. Egy 4 hosszú kör minden második csúcsa S-beli, minden második csúcsa T-beli lenne. Azonban ekkor a két S-beli csúcsnak két T-beli közös szomszédja is lenne, de a gráf konstrukciójából következően ez nem lehetséges. Ha pedig $x_1x_2x_3x_4x_5x_6x_7x_8x_1$ egy 8 hosszú kör lenne G_0-ban, ahol $x_1, x_3, x_5, x_7 \in S$, $x_2, x_4, x_6, x_8 \in T$, akkor $x_1x_3x_5x_7x_1$ egy 4 hosszú kör lenne H-ban, hiszen minden $i \in \{1, 3, 5, 7\}$ esetén x_i és x_{i+2} csúcsoknak x_{i+1} közös szomszédja G_0-ban ($x_9 := x_1$).

Térjünk rá G_0 éleinek vizsgálatára. A G_0 gráfban minden T-beli csúcs foka 0, vagy 2. Jelölje $T_1 \subseteq T$ a 0 fokú csúcsok, $T_2 \subseteq T$ pedig a 2 fokú csúcsok halmazát. A H-beli élek és a T_2-beli csúcsok közötti bijektív megfeleltetés miatt

$$|T_2| = |E(H)| \geq \frac{1}{3}\pi(n^{2/5}(\log n)^{1/5})^{3/2}.$$

Legyen G az a páros gráf, melyet úgy kapunk G_0-ból, hogy S-hez hozzávesszük az 1-et, és összekötjük a T_1-beli csúcsokkal. Vagyis a két független csúcsosztály $S \cup \{1\}$ és T lesz:

$$V(G) = S \cup \{1\} \cup T,$$

a gráf éleinek halmaza pedig

$$E(G) = E(G_0) \cup \{1x \mid x \in T_1\}.$$

Azt állítjuk, hogy az

$$A = \{xy \mid xy \in E(G)\}$$

halmaz kielégíti a feltételeket.

A konstrukcióból következik, hogy $A \subseteq \{1, 2, \ldots, n\}$, valamint, ha n elegendően nagy, akkor

$$|A| = |E(G)| = |T| + |T_2| \geq$$
$$\geq \pi(n) - \pi(n^{2/5}(\log n)^{1/5}) + \frac{1}{3}\pi(n^{2/5}(\log n)^{1/5})^{3/2} \geq$$
$$\geq \pi(n) + n^{3/5}/(\log n)^{6/5},$$

hiszen különböző G-beli xy élekre az xy szorzat is különböző. Belátjuk, hogy az

$$s_1 s_2 s_3 s_4 = t_1 t_2 t_3 t_4 \tag{5.19}$$

egyenletnek nincsen páronként különböző A-beli elemekből álló megoldása. Az A halmaznak egyetlen olyan eleme van, mely osztható a $p \in T_1$ prímszámmal: p. Ez azt jelenti, hogy ha p szerepelne valamelyik oldalon, akkor a másik oldalon is szerepelnie kellene, ami nem lehetséges. Ezért T_1-beli prímek az egyenlet egyik oldalán sem szerepelhetnek, vagyis az $s_1, s_2, s_3, s_4, t_1, t_2, t_3, t_4$ számok mind G_0-beli éleknek felelnek meg, azaz felírhatók egy-egy S-beli és egy-egy T_2-beli prímszám szorzataként. Ekkor, ha az (5.19) egyenlet fennáll, akkor a nekik megfelelő élhalmaz körök uniója. Mivel a gráf páros, ezért ez csak úgy lehetséges, ha két 4 hosszú kört, vagy egyetlen 8 hosszú kört alkotnak. Mivel G_0 nem tartalmaz sem C_4-et, sem C_8-at, ezért ez sem lehetséges. Ezzel bizonyítottuk az állítást.

□

Az 5.12. és 5.13. Tételekben G_4-re kapott alsó és felső becsléseket összefoglalva a következő eredményt kapjuk:

5.14. Következmény. *Tetszőleges $\varepsilon > 0$-ra létezik olyan $N = N(\varepsilon)$, hogy minden $n > N$ esetén teljesül a következő egyenlőtlenség:*

$$\pi(n) + n^{3/5}/(\log n)^{6/5} \leq G_4(n) \leq \pi(n) + (10 + \varepsilon)n^{2/3}.$$

5.4. Következmények

Erdős multiplikatív Sidon-sorozatok elemszámáról a következő tételt bizonyította:

Tétel (Erdős, [11]). Léteznek olyan C_1, C_2 pozitív konstansok, amelyekkel teljesül az

$$\pi(n) + C_1 \frac{n^{3/4}}{(\log n)^{3/2}} \leq G_2(n) \leq \pi(n) + C_2 \frac{n^{3/4}}{(\log n)^{3/2}}$$

egyenlőtlenség.

Most Erdős eredményét felhasználva az 5.11. és 5.12. Tételek segítségével már tetszőleges k-ra érvényes becsléseket igazolunk.

5.15. Következmény. *Legyen $3 \leq k$ pozitív egész szám, és legyen $\varepsilon > 0$ tetszőleges. Ekkor létezik olyan $N = N(\varepsilon)$, mellyel minden $N < n$ esetén teljesül a*

$$G_k(n) \leq \pi(n) + (c_k + \varepsilon)n^{2/3},$$

egyenlőtlenség, ha k páros, illetve a

$$G_k(n) \leq \pi(n) + \pi(n/2) + (c_k + \varepsilon) \cdot n^{2/3} \cdot \frac{\log n}{\log\log n},$$

egyenlőtlenség, ha k páratlan. Itt $c_4 = 10$, $c_6 = 6$, ha $6 < k$ páros szám, akkor $c_k = k - 3$, ha pedig $3 \leq k$ páratlan szám, akkor $c_k = \frac{2e}{3}$.

Bizonyítás. Az 5.12. Tétel szerint az állítás páros k esetén teljesül.

Páratlan k-ra az állítást teljes indukcióval bizonyítjuk. Az 5.11. Tétel szerint $k = 3$ esetén az állítás teljesül. Tegyük fel, hogy a $k \geq 3$ páratlan számra már igazoltuk az állítást. Azaz minden $\varepsilon > 0$-ra létezik olyan $N_k = N_k(\varepsilon)$ korlát, hogy $n > N_k$ esetén, ha az $A \subseteq \{1, 2, \dots, n\}$ halmazra teljesül, hogy

$$|A| \geq \pi(n) + \left(\frac{2e}{3} + \varepsilon\right) n^{2/3} \frac{\log n}{\log\log n},$$

akkor A-nak kiválasztható $2k$ különböző eleme, melyekre $s_1 \dots s_k = t_1 \dots t_k$. Legyen most $n > N_k$, $A \subseteq \{1, 2, \dots, n\}$, és tegyük fel, hogy

$$|A| \geq \pi(n) + \pi(n/2) + \left(\frac{2e}{3} + \varepsilon\right) n^{2/3} \frac{\log n}{\log\log n}.$$

Ha n elég nagy, akkor ebből következik, hogy

$$|A| \geq \pi(n) + \pi(n/2) + \left(\frac{2e}{3} + \varepsilon\right) n^{2/3} \cdot \frac{\log n}{\log\log n} \geq$$
$$\geq \pi(n) + C_2 n^{3/4}/(\log n)^{3/2},$$

és így Erdős eredménye szerint az

$$s_{k+1}s_{k+2} = t_{k+1}t_{k+2}$$

egyenletnek van A-ban páronként különböző számokból álló megoldása. Rögzítsünk egy ilyen megoldást. Az $A \setminus \{s_{k+1}, s_{k+2}, t_{k+1}, t_{k+2}\}$ halmazra alkalmazva az indukciós feltevést, elegendően nagy n esetén kiválasztható $2k$ páronként különböző eleme, melyekre

$$s_1 \dots s_k = t_1 \dots t_k.$$

Az $s_1, \dots, s_{k+2}, t_1, \dots, t_{k+2}$ számok páronként különbözők, és

$$s_1 \dots s_{k+2} = t_1 \dots t_{k+2},$$

így $k + 2$-re is igazoltuk az állítást. Ezzel a tételt igazoltuk.

□

Erdős, Sárközy és T. Sós azt vizsgálták, hogy az $\{1, 2, \dots, n\}$ halmaznak legfeljebb hány eleme választható ki úgy, hogy közülük semelyik $2k$ különbözőnek a szorzata ne legyen négyzetszám. Az ilyen tulajdonságú halmazok maximális $F_{2k}(n)$ elemszámáról a következő tételt bizonyították:

Tétel (Erdős, Sárközy, T. Sós, [12]). Legyen $1 < k$ pozitív egész szám. Létezik olyan $c > 0$ konstans, hogy teljesülnek a következő egyenlőtlenségek:

$$F_{2k}(n) \le \pi(n) + cn^{3/4}/(\log n)^{3/2},$$

ha k páros, és n elég nagy, illetve

$$F_{2k}(n) \le \pi(n) + \pi(n/2) + cn^{7/9}\log n,$$

ha k páratlan, és n elég nagy.

Az 5.15. Következményt felhasználva Erdős, Sárközy és T. Sós eredményénél erősebb állítást tudunk igazolni:

5.16. Következmény. *Legyen $3 \le k$ pozitív egész szám, és legyen $\varepsilon > 0$ tetszőleges. Ekkor létezik olyan $N = N(\varepsilon)$, mellyel minden $N < n$ esetén teljesül a*

$$F_{2k}(n) \le \pi(n) + (c_k + \varepsilon)n^{2/3},$$

egyenlőtlenség, ha k páros, illetve a

$$F_{2k}(n) \leq \pi(n) + \pi(n/2) + (c_k + \varepsilon) \cdot n^{2/3} \cdot \frac{\log n}{\log\log n},$$

egyenlőtlenség, ha k páratlan. Itt $c_4 = 10$, $c_6 = 6$, ha $6 < k$ páros szám, akkor $c_k = k - 3$, ha pedig $3 \leq k$ páratlan szám, akkor $c_k = \frac{2e}{3}$. egyenlőtlenség, ha k páratlan.

Bizonyítás. Ha az

$$s_1 \dots s_k = t_1 \dots t_k \ (s_1 \dots, s_k, t_1, \dots, t_k \in A)$$

egyenletnek létezik páronként különböző számokból álló megoldása, akkor $x = s_1 \dots s_k$, $s_{k+i} = t_i$ az

$$s_1 \dots s_{2k} = x^2$$

egyenlet egy megoldását adják. Ezért $F_{2k}(n) \leq G_k(n)$ minden n-re teljesül. Így az állítás közvetlenül következik az 5.15. Következményből.

□

Megjavítjuk Erdős, Sárközy és T. Sós alsó becslését $F_8(n)$-re. Ők $F_8(n) \geq \pi(n) + cn^{5/9}/(\log)^{10/9}$ egyenlőtlenséget igazolták, mi a hibatagban n kitevőjét 3/5-re növeljük.

5.17. Következmény. *Ha n elegendően nagy, akkor teljesül a következő egyenlőtlenség:*

$$F_8(n) \geq \pi(n) + n^{3/5}/(\log n)^{6/5}.$$

Bizonyítás. Az 5.13. Tételben szereplő konstrukció ennél a problémánál is megfelelő. Az ott szereplő bizonyítás kis módosítással itt is alkalmazható. □

Sokat vizsgált kérdés, hogy egy $A \subseteq \mathbb{N}$ Sidon-sorozat esetén hogyan viselkedik, mennyire „nagy" lehet az $|A(n)| = |A \cap \{1, 2, \dots, n\}|$ sorozat. Erdős [20] megmutatta, hogy létezik olyan c konstans, mellyel tetszőleges A additív Sidon-sorozatra teljesül, hogy $\liminf_{n\to\infty} |A(n)|/\sqrt{n/\log n} \leq c$. Azonban egy rögzített n-re $\{1, 2, \dots, n\}$-ben akár aszimptotikusan $\sqrt{n}$ méretű Sidon-sorozat is konstruálható. Ajtai, Komlós és Szemerédi [1] olyan $A \subseteq \mathbb{N}$ additív Sidon-sorozat létezését igazolták, melyre minden elegendően nagy n esetén fennáll az $|A(n)| > 10^{-3}(n \log n)^{1/3}$ egyenlőtlenség. Ezt az eredményt Ruzsa [38] megjavította, és olyan additív Sidon-sorozatot konstruált, melyre minden elegendően nagy n esetén teljesül, hogy $|A(n)| > n^{\sqrt{2}-1-o(1)}$. Megmutatjuk, hogy a mi általunk vizsgált problémánál az $|A(n)|$ elemszám aszimptotikusan akkora is lehet, mintha csak egyetlen rögzített n esetén vennénk $\{1, 2, \dots, n\}$-ben egy feltételeket kielégítő sorozatot. Mint láttuk, az additív esetben ez nem igaz, ott ez a nagyságrend nem érhető el.

5.18. Következmény. *Legyen $2 < k \in \mathbb{N}$. Tegyük fel, hogy az $A \subseteq \mathbb{N}$ halmazra teljesül, hogy az*

$$s_1 \dots s_k = t_1 \dots t_k \ (s_1, \dots, s_k, t_1, \dots, t_k \in A) \tag{5.20}$$

egyenletnek nincsen páronként különböző számokból álló megoldása. Ekkor létezik olyan c_k konstans, mellyel a következő becslések érvényesek:

$$|A(n)| \le \pi(n) + c_k n^{2/3}, \qquad \textit{ha } k \textit{ páros és } n \textit{ elég nagy,}$$

$$|A(n)| \le \pi(n) + \pi(n/2) + c_k n^{2/3} \frac{\log n}{\log\log n}, \qquad \textit{ha } k \textit{ páratlan és } n \textit{ elég nagy.}$$

Továbbá létezik olyan $A \subseteq \mathbb{N}$, amelyre az (5.20) *egyenletnek nincsen páronként különböző számokból álló megoldása, továbbá*

$$|A(n)| \ge \pi(n) + \pi(n/2) - 2, \ \textit{ha } k \textit{ páratlan, illetve}$$

$$|A(n)| \ge \pi(n), \ \textit{ha } k \textit{ páros}$$

minden n-re teljesül.

Bizonyítás. Az 5.15. Következmény miatt az állítás első fele teljesül páratlan és páros k esetén is.

Az állítás második felének igazolásához először tegyük fel, hogy k páros. A számelmélet alaptételéből következik, hogy

$$A = \{p \mid p \le n \text{ és } p \text{ prím}\}$$

esetén (5.20) csak úgy teljesülhet, ha

$$\{s_1, \dots, s_k\} = \{t_1, \dots, t_k\}.$$

Ebből következik, hogy az A halmaz kielégíti a feltételt, az elemszáma pedig

$$|A| = \pi(n).$$

Végül, legyen $k > 1$ páratlan szám. Megmutatjuk, hogy

$$A = \{p \mid 2 < p \leq n \text{ és } p \text{ prím}\} \cup \{2q \mid 2 < q \leq n/2 \text{ és } q \text{ prím}\}$$

esetén a (5.20) egyenletnek nincsen páronként különböző számokból álló megoldása. Tegyük fel, hogy (5.20) teljesül az

$$s_1, \ldots, s_k, t_1, \ldots, t_k \in A$$

számokra. Az $s_1, \ldots, s_k$ számok indexelését megváltoztathatjuk úgy, hogy alkalmas j-vel az $s_1, \ldots, s_j$ számok páratlan prímszámok, az s_{j+1}, ..., s_k számok pedig páratlan prímszámok kétszeresei legyenek. Mivel egyik s_i sem szerepelhet a $t_1, \ldots, t_k$ számok között, ezért csak úgy állhatna fenn az (5.20) egyenlőség, ha teljesül, hogy

$$\{t_1, \ldots, t_k\} = \{2s_1, \ldots, 2s_j, s_{j+1}/2, \ldots, s_k/2\}.$$

Mivel az (5.20) egyenlet két oldalát a 2 egyforma hatványon osztja, ezért ebben az esetben $2^j = 2^{k-j}$ teljesülne, és így $k = 2j$ páros szám lenne, ami ellentmondás. Az A halmaz elemszáma

$$|A| = \pi(n) + \pi(n/2) - 2.$$

□

Jelölje $G'_k(n)$ legnagyobb olyan $A \subseteq \{1, 2, \ldots, n\}$ halmaz elemszámát, melyre az

$$a_1 \ldots a_k = b_1 \ldots b_k \ (a_1, \ldots, b_k \in A)$$

egyenlet összes megoldására $\{a_1, \ldots, a_k\} = \{b_1, \ldots, b_k\}$ teljesül. A $G'_k(n)$ sorozat az additív Sidon-sorozatok általánosításaként kapott $B_k[1]$-sorozat multiplikatív analogonja. Megmutatjuk, hogy a G_k-ra kapott felső becslésekből könnyen levezethetők G'_k-re vonatkozó felső becslések is.

5.19. Következmény. *Tetszőleges $\varepsilon > 0$ esetén létezik olyan $N = N(\varepsilon)$, hogy minden $N < n$ esetén*

$$G'_3(n) \leq \pi(n) + \pi(n/2) + \left(\frac{2e}{3} + \varepsilon\right) n^{2/3} \log n / \log\log n,$$

valamint tetszőleges $k \geq 4$ *esetén*

$$G'_k(n) \leq \pi(n) + (10 + \varepsilon)n^{2/3}$$

teljesül .

Bizonyítás. A G_k és G'_k sorozatok definíciójából következik, hogy $G'_k(n) \leq G_k(n)$ és $G'_k(n) \leq G'_{k-1}(n)$ is teljesül. Ennek a két észrevételnek a segítségével az 5.11. és 5.12. Tételekből az állítás már következik. □

Irodalomjegyzék

[1] M. Ajtai, J. Komlós, E. Szemerédi: *A dense infinite Sidon sequence*, European J. Comb. 2 (1981) 1–11.

[2] J. A. Bondy, M. Simonovits: *Cycles of even length in graphs*, J. Combinatorial Theory Ser. B 16 (1974) 97–105.

[3] D. de Caen, L. A. Székely: *On dense bipartite graphs of girth eight and upper bounds for certain configurations in planar point-line systems*, J. Combin. Theory Ser. A 77(2) (1997) 268–278.

[4] T. H. Chan: *On sets of integers, none of which divides the product of k others*, European J. Combin. 32 (3) (2011) 443–447.

[5] T. H. Chan, E. Győri, A. Sárközy: *On a problem of Erdős on integers, none of which divides the product of k others*, European J. Combin. 31 (1) (2010) 260–269.

[6] P. Csikvári, K. Gyarmati, A. Sárközy: *Density and Ramsey type results on algebraic equations with restricted solution sets*, Combinatorica, megjelenés alatt.

[7] P. Dusart: *The k^{th} prime is greater than $k(lnk + lnlnk - 1)$ for $k > 2$*, Math. Comp. 68 (1999) 411–415.

[8] R. Eggetsberger: *On constructing codes from planar nearrings*, http://www.algebra.uni-linz.ac.at/Nearrings/nrcodes.html

[9] P. Erdős: *On sequences of integers no one of which divides the product of two others and some related problems*, Tomsk. Gos. Univ. Učen. Zap. 2 (1938) 74–82.

[10] P. Erdős: *An asymptotic inequality in the theory of numbers*, Vestnik Leningrad Univ. 15 (1960) 41–49. (oroszul)

[11] P. Erdős: *On some applications of graph theory to number theoretic problems*, Publ. Ramanujan Inst. 1 (1969) 131–136.

[12] P. Erdős, A. Sárközy, V. T. Sós: *On the product representations of powers, I*, European J. Comb. 16 (1995) 567–588.

[13] Z. Füredi, A. Naor, J. Verstraëte: *On the Turán number for the hexagon*, Adv. Math. 203(2) (2006) 476–496.

[14] R. L. Graham, B. L. Rotschild, J. H. Spencer: *Ramsey Theory*, Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons (1990)

[15] K. Gyarmati: *On a problem of Diophantus*, Acta Arith. 97 (2001) 53–65.

[16] K. Gyarmati, A. Sárközy: *Equations in finite fields with restricted solution sets, I. (Character sums)*, Acta Math. Hungar. 118 (2008) 129–148.

[17] K. Gyarmati, A. Sárközy: *Equations in finite fields with restricted solution sets, II. (Algebraic equations)*, Acta Math. Hungar. 119 (2008) 259–280.

[18] E. Győri: *C_6-free bipartite graphs and product representation of squares*, Discrete Math. 165/166 (1997) 371–375.

[19] L. Hajdu, A. Schinzel, M. Skałba: *Multiplicative properties of sets of positive integers*, Arch. Math. 93 (2009) 269–276.

[20] H. Halberstam, K. F. Roth: *Sequences*, Springer-Verlag, second edition (1983)

[21] N. Hindman: *Monochromatic sums equal to products in* $\mathbb{N}$, Integers 11A (2011) 1–10.

[22] P.-Y. Huang, W.-F. Ke, G. Pilz: *The cardinality of some symmetric differences*, Proc. Amer. Math. Soc. 138 (2010) 787–797.

[23] E. Landau: *Handbuch der Lehre von der Verteilung der Primzahlen*, vol. 1, Leipzig (1909).

[24] B. M. Landman, A. Robertson: *Ramsey Theory on the Integers*, American Mathematical Society (2003)

[25] A. Naor, J. Verstraëte: *A note on bipartite graphs without $2k$-cycles*, Probability, Combinatorics and Computing 14(5-6) (2005) 845–849.

[26] P. P. Pach: *The Ramsey-type version of a problem of Pomerance and Schinzel*, Acta Arith., megjelenés alatt (2012).

[27] P. P. Pach: *Ramsey type results on the solvability of certain equations in $\mathbb{Z}_m$*, Integers, beküldve (2012).

[28] P. P. Pach, G. Pluhár, A. Pongrácz, Cs. Szabó: *Multiplicative Sidon sequences*, kézirat.

[29] P. P. Pach, Cs. Szabó: *On the minimal distance of near-ring codes*, DMTCS 13(4) (2011) 33–44.

[30] G. Pilz: *Near-Rings*, North-Holland Publishing Company (1983)

[31] G. Pilz: *Near-rings: What they are and what they are good for*, http://www.algebra.uni-linz.ac.at/Nearrings/what-are.html

[32] G. Pilz: *On polynomial near-ring codes*, Contributions to general algebra 8, Verlag Hölder-Pichler-Tempsky, Wien (1992) 233–238.

[33] C. Pomerance, A. Schinzel: *Multiplicative properties of sets of residues*, Moscow J. Combin. and Number Theory 1 (2011) 52–66.

[34] R. Rado: *Studien zur Kombinatorik*, Math. Z. 36(1) (1933) 424–470.

[35] I. Reiman: *Über ein Problem von K. Zarankiewicz*, Acta. Math. Acad. Sci. Hung. 9 (1959) 269–279.

[36] G. Robin: *Estimation de la fonction de Tschebyshef ϑ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$, nombre de diviseurs premiers de n*, Acta. Arith., 42(4) (1983) 367–389.

[37] J. B. Rosser, L. Schoenfeld: *Approximate formulas for some functions of prime numbers*, Ill. Journ. Math. 6 (1962) 64–94.

[38] I. Ruzsa: *An infinite Sidon sequence*, Journal of Number Theory (68)1 (1998) 63–71.

[39] A. Sárközy: *On products and shifted products of residues modulo p*, Integers 8 (2008) 8 oldal.

[40] A. Sárközy: *On sums and products of residues modulo p*, Acta Arith. 118 (2005) 403–409.

[41] I. Schur: *Über die Kongruenz $x^m+y^m = z^m$ (mod p)*, Jahresber Deutsch. Math. Verein. 25 (1916) 114–117.

[42] E. Szemerédi: *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. 27 (1975) 199–245.

[43] B. L. van der Waerden: *Beweis einer Baudetschen Vermutung*, Nieuw. Arch. Wisk. 15 (1927) 212–216.

Összefoglalás

A dolgozatban olyan multiplikatív számelméleti kérdésekkel foglalkozunk, amelyek nagy részében fontos szerepet játszik, hogy bizonyos halmazokban hány elem áll elő pontosan egyféleképpen, mint szorzat.

Először Pilz egy kódelméleti eredetű sejtését igazolva megmutatjuk, hogy a $K \cdot \{1, 2, \ldots, n\}$ szorzatban páratlan sokszor szereplő elemek száma legalább n, ha $K = \{1, 2, \ldots, k\}$. Az eddig ismert becsléseket megjavítva bebizonyítjuk, hogy tetszőleges $K \subseteq \mathbb{N}$ esetén ezeknek az elemeknek a száma legalább $n/(\log n)^{0,223}$.

A következő két fejezetben egyenletek megoldhatóságára vonatkozó Ramsey-típusú és sűrűségi tételeket bizonyítunk. Pomerance és Schinzel kérdését megválaszolva igazoljuk, hogy a négyzetmentes számok tetszőleges r-színezése esetén van monokromatikus megoldása az $a_1 \ldots a_k = b_1 \ldots b_l$ egyenletnek. Csikvári, Gyarmati és Sárközy azt kérdezték, hogy igazolható-e Ramsey-típusú eredmény az $a + b = cd$ és $ab + 1$ egyenletek $\mathbb{Z}_m$-beli megoldhatóságáról. Mi megmutatjuk, hogy általánosabban, az $a_1 + \cdots + a_n = cd$ egyenlet esetén is igaz Ramsey-típusú eredmény $\mathbb{Z}_m$-ben, az $ab + 1 = cd$ egyenlet esetén viszont nem. Megfogalmazunk egy új feltételt, amely mellett sűrűségi tételt adunk az $ab + 1 = cd$ egyenlet $\mathbb{Z}_m$ feletti megoldhatóságára.

Az utolsó fejezetben a multiplikatív Sidon-sorozatok általánosításaként azt vizsgáljuk, hogy az $\{1, 2, \ldots, n\}$ számok közül legfeljebb hányat lehet úgy kiválasztani, hogy az $a_1 \ldots a_k = b_1 \ldots b_k$ egyenletnek ne legyen páronként különböző számokból álló megoldása. Ezt a maximális elemszámot aszimptotikus pontossággal meghatározzuk: páratlan k esetén $\pi(n) + \pi(n/2)$, páros k esetén $\pi(n)$. Erdős, Sárközy és T. Sós, valamint Győri azt a rokon problémát vizsgálták, hogy hány szám választható ki úgy, hogy közülük semelyik $2k$-nak a szorzata ne legyen négyzetszám. A becsléseink következményeként, illetve konstrukció segítségével az ő eredményeiket is megjavítjuk.

Summary

In this thesis several problems arising form multiplicative number theory are investigated.

In Section 2 we settle a 20 year old conjecture of Pilz originating from coding theory. We prove that the number of products that occur odd many times in $K \cdot \{1, 2, \ldots, n\}$ is at least n for $K = \{1, 2, \ldots, k\}$, where k is an arbitrary integer. Moreover, by improving the previously known bounds we show that the number of these elements is at least $n/(\log n)^{0,223}$ for any finite $K \subset \mathbb{N}$.

In Sections 3 and 4 certain equations with restricted solution sets are studied. Answering a question of Pomerance and Schinzel we prove that for any r-colouring of $\mathbb{N}$ the equation $a_1 \ldots a_k = b_1 \ldots b_l$ has a nontrivial monochromatic solution. Csikvári, Gyarmati and Sárközy asked whether there exist Ramsey-type results over $\mathbb{Z}_m$ for the equations $a + b = cd$ and $ab + 1 = cd$. We show that for any r-colouring of $\mathbb{Z}_m$ the even more general equation $a_1 + \cdots + a_n = cd$ has a nontrivial monochromatic solution. However, for the equation $ab + 1 = cd$ no Ramsey-type result can be stated. Therefore, we reformulate the problem adding an additional condition for the size of the prime divisors of m, and prove a density theorem for the solution of the equation under the new condition.

The topic of section 5 is generalizations of multiplicative Sidon-sets. We investigate the maximum number of elements that can be chosen from the set $\{1, 2, \ldots, n\}$ in such a way that the equation $a_1 \ldots a_k = b_1 \ldots b_k$ does not have a solution of distinct elements. As one of the main results of this thesis an asymptotically sharp bound is derived for this maximal number: $\pi(n) + \pi(n/2)$ for odd k and $\pi(n)$ for even k. Moreover, we improve a result of Erdős, Sárközy, T. Sós and Győri involving subsets of integers where no $2k$-element product can be a perfect square.